INTERNET LAW: SPRING 2010
PROFESSOR GRIMMELMANN
NEW YORK LAW SCHOOL

READING PACKET 2

ONLINE SPEECH

Contents

Class 8: Free Speech 3

Blown to Bits, ch. 7 4
Restatement (Second) of Torts 4
Twitter Problem 6
Blu-Ray Problem 6
United States v. Baker 7
Nuremberg Files problem 12

Class 9: Governmental Speech Regulation 14

Pornography Law primer 15
CDA Negotiation Problem 16
Reno v. ACLU 18
Pornography Law Problems 23

Class 10: Section 230 25

47 U.S.C. § 230 (excerpt) 26
Zeran v. America Online, Inc. 26
Blumenthal v. Drudge 32

Class 11: More Section 230 37

Doe v. Myspace, Inc. 38
Fair Housing Council v. Roommates.com, LLC 41
AutoAdmit Section 230 Problem 49

CLASS 8: FREE SPEECH

We're now ready for our first substantive topic, free speech. This is not a course in the First Amendment, so this won't be a detailed discussion of those (often quite intricate) doctrines. Instead, this class and the next one will present an impressionistic tour of a few issues that arise as we attempt to fit speech doctrine to the Internet. Today's class will focus on challenges of classifying online speech; next time's will focus on government attempts to regulate pornography. This setup, in turn, will lead into next week's classes on intermediary liability for the speech of users—a story whose history combines these two issues.

Preparation questions

(1) I'm starting you off with excerpts from the Restatement (Second) of Torts. I want you to meet the basic speech torts: intentional infliction of emotional distress (§ 46); defamation (§ §558–59, 577–78, 581); intrusion on seclusion (§ 652B); public disclosure of private facts (§ 625D); false light (§ 625E); and tortious interference with contract (§ 766). We'll return to them in the weeks to come, but for now, look at the balance the common law tried to strike. What personal and dignitary interests do these torts protect? How could tort liability harm free speech values? For each tort, what elements or limitations keep it from overly restricting speech?

(2) The Restatement is full of provisions that distinguish different media. (See, for example, § 581(2) on television and radio.) The Internet, however, is famously capable of behaving like all sorts of different media. In media circles, this phenomenon is known as *convergence*. It's a big problem for any body of law that tries to treat different media differently. Why? Does Twitter seem more like a letter, a telephone conversation, a newspaper, a public speech, or a television broadcast? How does your answer affect your conclusion as to whether Bonnen is potentially liable?

(3) In the Blu-Ray problem, you probably haven't yet learned about balancing the First Amendment with intellectual property rights. But don't let that stop you! Take it for granted that if someone stole the the secret formula to Coca-Cola and handed it to you, you wouldn't get very far arguing that you had a free speech right to distribute it to the world. The problem asks you to consider what happens to that principle on the Internet. Identify the distinctive challenges posed by each of the three users. Why does the Internet make these challenges worse for copyright and trade secret owners? How are free speech values implicated?

(4) On one level, the Jake Baker case is about "true threat" doctrine. On that level, it should provide you with the guidance you need to answer the Nuremberg Files problem, which is also about online threats. What do these two cases have in common? What differentiates them? What is the relevant holding in the Baker case, and how does it apply to Horsley? Can you think of a narrow reading of Baker that would allow the suit against Horsley to proceed, and a broad reading that would allow Horsley to prevail? Which is more persuasive? Why?

(5) But the Baker case—and indeed all the readings for today—also raise a larger question. Is speech on the Internet somehow different? One possible argument comes from John Perry Barlow: the Internet is *all speech*. Think about it. What's the worst thing someone could do to you offline? And online? How does this play into Barlow's argument that governments

should keep their hands off the Internet? And go back to Goldsmith and Wu: how many of their examples depend on the movement of physical *things*, like Nazi memorabilia? If we're *only* talking about speech, do their arguments lose any of their force? Should Amanda Bonnen be immune from liability because what she said was only a tweet, not some kind of offline conduct that really matters?

(6) Perhaps it's the opposite. Is speech on the Internet perhaps *worse* than offline speech? Why might that be? What harms would Amanda Bonnen, Jake Baker, and Neal Horsley been able to cause in a purely offline world? How about some of our favorites from past classes: Dow Jones (in *Gutnick*) and the New Haven Advocate (in *Young*)? Do we perhaps need to be less speech-protective, now that words can spread so far so fast?

(7) The Jake Baker prosecution failed. Does that mean he's off the hook? What about the classmate whose name he used in the rape-murder fantasy he posted to alt.sex.stories? [You can think of alt.sex.stories, a "USENET newsgroup," as being like a publicly accessible web bulletin board. The full story is reprinted in the dissenting opinion in *United States v. Alkhabaz*, 104 F.3d 1492, 1497 n.1 It's extremely unpleasant and I recommend not looking at it if you want to feel good about humanity.] Does she have any potential recourse?

BLOWN TO BITS, ch. 7

Please read chapter 7 of *Blown to Bits*.

Restatement (Second) of Torts

§ 46 Outrageous Conduct Causing Severe Emotional Distress

(1) One who by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another is subject to liability for such emotional distress, and if bodily harm to the other results from it, for such bodily harm. ...

§ 558 Elements Stated

To create liability for defamation there must be:

(a) a false and defamatory statement concerning another;

(b) an unprivileged publication to a third party;

(c) fault amounting at least to negligence on the part of the publisher; and

(d) either actionability of the statement irrespective of special harm or the existence of special harm caused by the publication. [JG: You can ignore (d) for now, but you'll eventually need to learn these rules when you study for the bar exam.]

§ 559 Defamatory Communication Defined

A communication is defamatory if it tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him.

§ 577 What Constitutes Publication

(1) Publication of defamatory matter is its communication intentionally or by a negligent act to one other than the person defamed.

(2) One who intentionally and unreasonably fails to remove defamatory matter that he knows to be exhibited on land or chattels in his possession or under his control is subject to liability for its continued publication.

§ 578 Liability of Republisher

Except as to those who only deliver or transmit defamation published by a third person, one who repeats or otherwise republishes defamatory matter is subject to liability as if he had originally published it.

§ 581 Transmission of Defamation Published by Third Person

(1) Except as stated in subsection (2), one who only delivers or transmits defamatory matter published by a third person is subject to liability if, but only if, he knows or has reason to know of its defamatory character.

(2) One who broadcasts defamatory matter by means of radio or television is subject to the same liability as an original publisher.

§ 652B Intrusion Upon Seclusion

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

§ 652D Publicity Given to Private Life

One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that

(a) would be highly offensive to a reasonable person, and

(b) is not of legitimate concern to the public.

§ 652E Publicity Placing Person in False Light

One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if

(a) the false light in which the other was placed would be highly offensive to a reasonable person, and

(b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.

comment b:

... 3: A is a renowned poet. B publishes in his magazine a spurious inferior poem, signed with A's name. Regardless of whether the poem is so bad as to subject B to liability for [defamation], B is subject to liability to A for [false light].

§ 766 Intentional Interference with Performance of Contract by Third Person

One who intentionally and improperly interferes with the performance of a contract (except a contract to marry) between another and a third person by inducing or otherwise causing the third person not to perform the contract, is subject to liability to the other for the pecuniary loss resulting to the other from the failure of the third person to perform the contract.

comment c: ... Thus physical violence, fraudulent misrepresentation and threats of illegal conduct are ordinarily wrongful means and subject their user to liability even though he is free to accomplish the same result by more suitable means. A, C's competitor for B's business, may justifiably induce B by permissible means not to buy from C ... ; he is not justified in doing so by the predatory means stated above. ...

Twitter Problem

For more on this story, *see, e.g.*, *Defamation Lawsuit for US Tweeter,* BBC NEWS (July 29, 2009). Amanda Bonnen used Twitter. On May 12, 2009, she tweeted:

> "@JessB123 You should just come anyway. Who said sleeping in a moldy apartment was bad for you? Horizon realty thinks it's okay."

(1) Horizon Group Management is her former landlord. Does it have sufficient grounds to file suit for defamation? For any other torts?

(2) Some commentators have argued that the tort of defamation is outdated in the digital world and should be abolished. They claim that Horizon can now take to the Internet to tell its side of the story, so it doesn't need legal remedies. Do you agree? Why or why not?

Blu-Ray Problem

This problem is based on *DVD Copy Control Ass'n, Inc. v. Bunner*, 75 P. 3d 1 (Cal. 2003), on *Universal City Studios, Inc. v. Corley*, 273 F.2d 429 (2d Cir. 2001), and on a well-publicized incident involving the users of Digg.com.

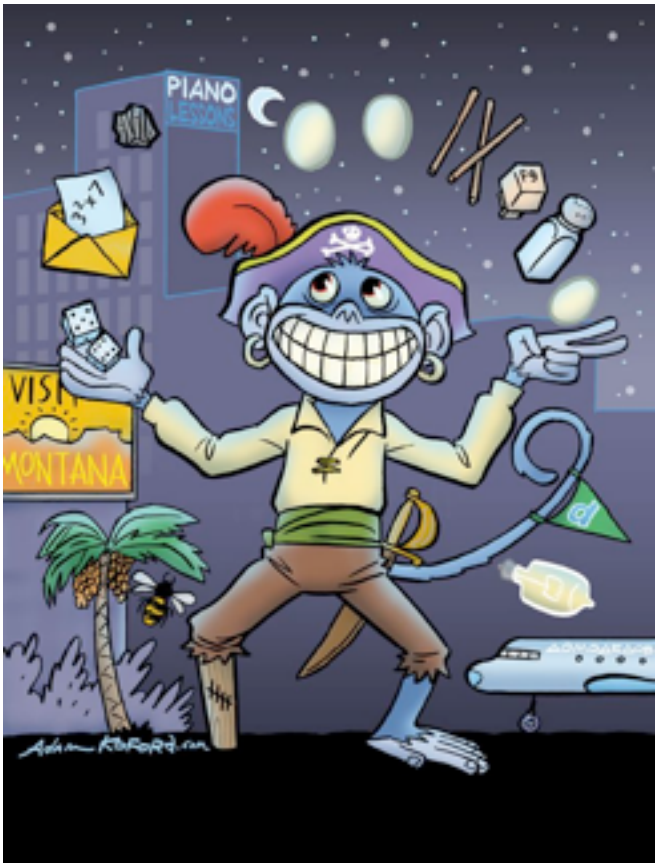
Blu-Ray discs and players use a copy protection technology known as AACS. Each Blu-Ray disc is encrypted, so that it appears to contain only a large sequence of random bits. An authorized Blu-Ray player, however, can use a secret "processing key" to decrypt the sequence of bits into a viewable movie. AACS Licensing Administrator ("AACS LA"), the organization that controls the AACS standard, gives out processing keys to Blu-Ray player manufacturers, and requires them to sign licensing agreements that (a) restrict what their players will do (e.g. no burning unencrypted copies of Blu-Ray discs) and (b) promise to keep the processing key secret.

It now appears that a processing key has leaked. An unknown user by the username of BluRazor has managed to extract the processing key from a Magnavox Blu-Ray player. He posted the key, the thirty-two-digit hexadecimal number 09-F9-11-02-9D-74-E3-5B-D8-41-56-C5-63-56-88-C0, to the DVD Technical Forum, a web discussion board for digital video programmers. Three days later, AACS LA sued the DVD Technical Forum and BluRazor for breach of trade secrecy and violation of Section 1201 of the Copyright Act, which prohibits "trafficking" in "devices" designed to facilitate copyright infringement by disabling "technological protection measures." (We'll discuss this section in more detail later in the course.) The Forum

and BluRazor immediately agreed to the entry of an injunction preventing them from distributing the processing key. The Forum replaced the post with a brief note that read, "This post has been deleted at the request of the AACS LA."

Hundreds of DVD Technical Forum users, however, had already seen the post, and were furious at what they saw as censorship of their community. Some of them had copied down the number. It wasn't long before three things happened:

(1) Dozens of users reposted the number in threads all across the DVD Technical Forum. These posts were deleted as soon as the Forum's administrators noticed them.



(2) A user with the Forum username DVD Monkey created his own site on the controversy. Considering it ridiculous that anyone could try to "own" a number, he created and posted this image. Here's a partial explanation of the symbolism:

> Beginning at the top, with the goose egg on the right, then proceeding clockwise we see a roman numeral. Next up is a function key. Then there's salt (I wonder what the atomic weight of sodium is?) followed by another goose egg. The monkey's holding up a couple of fingers, and his tail is making a funny shape too! What's that on the flag? Down from there we see a tungsten bulb (again, what's the atomic weight of tungsten?). ...

(3) Also outraged at the AACS LA's actions, a self-proclaimed "hacker activist" who goes by the pseudonym Winston Smithereens has created a collection of links to every place on the Internet where the number can be found, including at the Forum and at DVD Monkey's site. So far, the list has about a hundred entries.

The AACS LA is weighing its next steps. They've called you for legal advice. What can they do? Can they put the monkeys back in the barrel, or have the DVD Technical Forum's users made a monkey out of Blu-Ray security?

United States v. Baker
890 F. Supp. 1375 (E.D. Mich. 1995)

COHN, District Judge.

...

I. Introduction

This is a criminal prosecution under 18 U.S.C. § 875(c). Defendant Jake Baker (Baker) is charged in a superseding indictment with five counts of transmitting threats to injure or kidnap another, in electronic mail (e-mail) messages transmitted via the Internet. Now before the Court is Baker's motion to quash the superseding indictment. For the reasons that follow, the motion will be granted.

II. Background

The e-mail messages that form the basis of the charges in this case were exchanged in December, 1994 between Baker in Ann Arbor, Michigan, and defendant Arthur Gonda (Gonda), who sent and received e-mail through a computer in Ontario, Canada. Gonda's identity and whereabouts are unknown. The messages excerpted in the superseding indictment are drawn from a larger e-mail exchange between Gonda and Baker began on November 29, 1994, and ended on January 25, 1995. The specific language of the messages excerpted in the superseding indictment will be discussed in detail below. They all express a sexual interest in violence against women and girls.

Baker first appeared before a United States Magistrate Judge on a criminal complaint alleging violation of 18 U.S.C. § 875(c), on February 9, 1995. The complaint was based on an FBI agent's affidavit which cited language taken from a story Baker posted to an Internet newsgroup entitled "alt.sex.stories," and from e-mail messages he sent to Gonda. The story graphically described the torture, rape, and murder of a woman who was given the name of a classmate of Baker's at the University of Michigan. The "alt.sex.stories" newsgroup to which Baker's story was posted is an electronic bulletin board, the contents of which are publicly available via the Internet. Much of the attention this case garnered centered on Baker's use of a real student's name in the story. The e-mail messages exchanged between Gonda and Baker were private, and not available in any publicly accessible portion of the Internet. ...

On March 15, 1995, the government charged Baker and Gonda in a superseding indictment with five counts of violating 18 U.S.C. § 875(c). The story on which the initial complaint was partially based is not mentioned in the superseding indictment, which refers only to e-mail messages exchanged between Gonda and Baker. The government has filed a bill of particulars identifying who it perceives to be the objects of the allegedly threatening transmissions, as well as witness and exhibit lists.

Baker, who is named in all five of the superseding indictment's counts, has filed a motion seeking dismissal of all the counts of the superseding indictment. He contends that application of 18 U.S.C. § 875(c) to the e-mail transmissions pushes the boundaries of the statute beyond the limits of the First Amendment. The government responds that the motion must be denied because the First Amendment does not protect "true threats," and because whether a specific communication constitutes a true threat is a question for the jury.

III. The Law

Eighteen U.S.C. § 875(c) reads:

> Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both.

The government must allege and prove three elements to support a conviction under § 875 (c): "(1) a transmission in interstate [or foreign] commerce; (2) a communication containing a threat; and (3) the threat must be a threat to injure [or kidnap] the person of another." ...

Because prosecution under 18 U.S.C. § 875(c) involves punishment of pure speech, it necessarily implicates and is limited by the First Amendment. Although the Supreme Court has not addressed the constitutionally permissible scope of § 875(c), it has considered a similar statute concerning threats against the President, 18 U.S.C. § 871(a),[in *Watts v. United States, 394 U.S. 705, 89 S.Ct. 1399, 22 L.Ed.2d 664.* ... Under *Watts,* to pass constitutional muster the government must initially prove "a true `threat.'" *Id.* ...

The only extended discussion of the constitutional dimension of the "true threat" requirement with regard to § 875(c) is found in *United States v. Kelner, 534 F.2d 1020 (2d Cir.), cert. denied,* 429 U.S. 1022, 97 S.Ct. 639, 50 L.Ed.2d 623 (1976). In *Kelner,* the Second Circuit drew on *Watts* to illuminate the constitutional limits of a prosecution under § 875(c):

> The purpose and effect of the *Watts* constitutionally-limited definition of the term "threat" is to insure that only unequivocal, unconditional and specific expressions of intention immediately to inflict injury may be punished — only such threats, in short, as are of the same nature as those threats which are ... "properly punished every day under statutes prohibiting extortion, blackmail and assault without consideration of First Amendment issues." *Watts,* 402 F.2d at 690. ...
>
> * * * * * *
>
> So long as the threat on its face and in the circumstances in which it is made is so unequivocal, unconditional, immediate and specific as to the person threatened, as to convey a gravity of purpose and imminent prospect of execution, the statute may properly be applied. This clarification of the scope of 18 U.S.C. § 875(c) is, we trust, consistent with a rational approach to First Amendment construction which provides for governmental authority in instances of inchoate conduct, where a communication has become "so interlocked with violent conduct as to constitute for all practical purposes part of the [proscribed] action itself."

Kelner, 534 F.2d at 1027 (quoting T. Emerson, The System of Freedom of Expression, 329 (1970)).

... Threats aimed at achieving some coercive end remain the typical subject of more contemporary cases. In *Cox,* for instance, the defendant's truck was repossessed while it contained items of his personal property. The defendant telephoned the bank that had had the truck repossessed and stated "I tell you what, you all better have my personal items to me by five o'clock today or it[']s going to be a lot of hurt people there." *Cox, 957 F.2d at 265.* The threat was designed to effect the return of the defendant's property, it targeted the people at the bank, and it was found not to be conditional (in part because his property could not have been returned by the five o'clock deadline). It falls within *Kelner's* requirement of a threat that is "so unequivocal,

unconditional, immediate and specific as to the person threatened, as to convey a gravity of purpose and imminent prospect of execution." 534 F.2d at 1027. ...

While coercive or extortionate threats are paradigmatic subjects of a prosecution under 18 U.S.C. § 875(c), a threat which is neither coercive nor extortionate may still satisfy the constitutional test from *Kelner,* indeed, *Kelner* itself involved a non-coercive threat to assassinate the PLO leader Yasser Arafat. *Kelner, 534 F.2d at 1025. See also, DeAndino, 958 F.2d at 146* (regarding threat that defendant was going to "blow [the victim's] brains out," and the victim was "going to die.") ...

IV. The Communications

... As the Court construes the law as discussed above, the constitutional standard enunciated in *Kelner* requires, at the very least, that a statement charged under § 875(c) contain some language construable as a serious expression of an intent imminently to carry out some injurious act. The language of the statement must be considered as it would be interpreted by the foreseeable recipients of the communication containing it. Statements expressing musings, considerations of what it would be like to kidnap or injure someone, or desires to kidnap or injure someone, however unsavory, are not constitutionally actionable under § 875(c) absent some expression of an intent to commit the injury or kidnapping. In addition, while the statement need not identify a specific individual as its target, it must be sufficiently specific as to its potential target or targets to render the statement more than hypothetical.

Before addressing the specific language quoted in the indictment, several observations pertain to all of the government's charges. First, all of the language for which Baker is charged was contained in private email messages he sent to Gonda. The messages were not available in any publicly accessible part of the Internet, and there is no allegation that they were ever distributed in any format, electronic or hardcopy, to anyone other than Gonda. Nothing in these private messages suggests that they would be further distributed. It is only as a result of this prosecution and the ensuing publicity that the content of the messages has been publicly aired.

The focus of the inquiry here, therefore, is how a reasonable person would expect Gonda to interpret the e-mail messages. Gonda's identity is entirely unknown; "he" could be a ten year old girl, an eighty year old man, or a committee in a retirement community playing the role of Gonda gathered around a computer. All that is known about Gonda is that he used a computer account based in Ontario, Canada, and that he apparently enjoyed exchanging with Baker what he referred to in an e-mail message dated January 3, 1995, as "REAL sex talk" concerning violence against women and girls. ...

B.

Counts II and III are based on the same statement made by Baker in an e-mail message dated December 9, 1994, and charge Baker with making a threat to kidnap and a threat to injure, respectively. The statement for which Baker is charged in the two counts reads:

> I just picked up Bllod Lust and have started to read it. I'll look for "Final Truth" tomorrow (payday). One of the things I've started doing is going back and re-reading earlier messages of yours. Each time I do. they turn me on more and more. I can't wait to see you in person. I've been trying to think of secluded spots. but my knowledge of

> Ann Arbor is mostly limited to the campus. I don't want any blood in my room, though I have come upon an excellent method to abduct a bitch —
>
> As I said before, my room is right across from the girl's bathroom. Wiat until late at night. grab her when she goes to unlock the dorr. Knock her unconscious. and put her into one of those portable lockers (forget the word for it). or even a duffle bag. Then hurry her out to the car and take her away ... What do you think?

The bill of particulars identifies the target of the statement as: "Female college students who lived in Defendant Jake Baker's dormitory at the University of Michigan in Ann Arbor, Michigan." Apart from concerns about equating Baker's online persona with his real person, the class of would-be targets here is identified with sufficient specificity.

Presumably, the government offers this statement as a threat to carry out the "method to abduct" it describes. Under *Kelner,* discussion of a method of kidnapping or injuring a person is not punishable unless the statement includes an unequivocal and specific expression of intention immediately to carry out the actions discussed. Baker's e-mail message cannot reasonably be read as satisfying this standard. As in Count I, the language with which Baker is charged here lacks any expression of an intention to act, and concludes with a request for Gonda's reaction: "What do you think?" Discussing the commission of a crime is not tantamount to declaring an intention to commit the crime. To find an expression of unequivocal intention in this language would require the drawing of an inference not grounded in any specific language of the statement and would exceed the bounds of the First Amendment. Counts II and III must be dismissed.

C.

Count IV charges Baker and Gonda with transmitting a threat to injure. The Count is based on a message from Gonda to Baker, and Baker's response. Both e-mail messages are dated December 10, 1994. Gonda wrote:

> Hi Jake. I have been out tonight and I can tell you that I am thinking more and more about `doing' a girl. I can picture it so well ... and I can think of no better use for their flesh. I HAVE to make a bitch suffer!
>
> As far as the Teale-homolka killings, well I can think of no tastier crimes ... BTW have you seen any pictures of the girls? You have to see these cunts! They must have been so much fun ... please let me know any details that I cannot get here. I would love to see what you think about it....
>
> As far as the asian bitch story, there is only one possible ending....

Baker responded:

> Are tastes are so similar. it scares me :-) When I lay down at night. all I think of before I sleep is how I'd torture a bitch I get my hands on. I have some pretty vivid near dreams too. I wish I could remember them when I get up.

The bill of particulars identifies the target of these statements as:

> Women who were the subject of Defendant Jake Baker's E-mail transmissions and Internet postings, including — but not limited to — Jane Doe, whose true name is known to Defendant Jake Baker and this Honorable Court.

This Count presents the weakest of all the government's charges against Baker. While the government identifies the class of targets here as women Baker discussed on the Internet, there is nothing in the language quoted here to so limit the class. In addition, since Baker's e-mail often refers simply to "a girl," a class composed of women Baker discussed in his e-mail and stories essentially is a class composed of any woman or girl about whom Baker has ever thought. Such a class is obviously not sufficiently specific.

With regard to the content of Baker's communication, Baker's statement here consists only of an expression of his thoughts before sleeping and of "near dreams" he cannot remember upon waking. To infer an intention to act upon the thoughts and dreams from this language would stray far beyond the bounds of the First Amendment, and would amount to punishing Baker for his thoughts and desires. Count IV must be dismissed. ...

V. Coda

... Baker is being prosecuted under 18 U.S.C. § 875(c) for his use of words, implicating fundamental First Amendment concerns. Baker's words were transmitted by means of the Internet, a relatively new communications medium that is itself currently the subject of much media attention. The Internet makes it possible with unprecedented ease to achieve world-wide distribution of material, like Baker's story, posted to its public areas. When used in such a fashion, the Internet may be likened to a newspaper with unlimited distribution and no locatable printing press — and with no supervising editorial control. But Baker's e-mail messages, on which the superseding indictment is based, were not publicly published but privately sent to Gonda. While new technology such as the Internet may complicate analysis and may sometimes require new or modified laws, it does not in this instance qualitatively change the analysis under the statute or under the First Amendment. Whatever Baker's faults, and he is to be faulted, he did not violate 18 U.S.C. § 875(c). The case would have been better handled as a disciplinary matter, as the University of Victoria proceeded in a similar situation, despite whatever difficulties inhere in such a course. ...

Nuremberg Files problem

This problem is based, with some tweaks, on *Planned Parenthood v. Amer. Coalition of Life*, 290 F. 3d 1058 (9th Cir. 2002).

Anti-abortion activist Neal Horsley operates a website called the "Nuremberg Files" that features the names of doctors who perform abortions, along with their spouses, pro-choice politicians, and judges who have ruled in ways Horsley Many of the names are accompanied by home addresses, license plate numbers, and photographs. Beneath each picture, in an Old West-style font, appears the logo "WANTED." After the murders of several doctors who performed abortions, Horsley put a strikethrough through their names. A legend at the top of the web page explains, ""Black font (working); Greyed-out Name (wounded); Strikethrough (fatality)."

An association of doctors who perform abortions and whose names appear on the Nuremberg Files website have sued Horsley under the federal Freedom of Access to Clinics Entrances (FACE) Act, which gives a makes it a crime to "[by] threat of force ... intentionally... intimidate[] ... any person because that person is or has been ... providing reproductive health services [including abortions]." 18 U.S.C. § 248(a)(1). FACE gives a private right of action to

"[a]ny person aggrieved by reason of the conduct prohibited" by the Act, including damages and injunctive relief. *Id.* § (c)(1).

The doctors have moved for a preliminary injunction requiring Horsley to remove the Nuremberg Files from the Internet. How should the court rule?

CLASS 9: GOVERNMENTAL SPEECH REGULATION

Today, we turn to the problem that historically all but defined the first generation of mass Internet activism. (There were computer *causes celebres* before, but this was the first real Internet-wide moment of political awakening.) This is the stuff that got John Perry Barlow up in arms—government attempts to squelch out pornography online.

The materials today walk you through a decade in Internet history, through the lens of Netizens' attempts to fight back against what they saw as clumsy anti-porn legislation. We start with a quick primer on the Supreme Court's porn jurisprudence; you should refer back to it regularly as you read the rest of the day's assignment. Next, there's a negotiation exercise to help you understand the political climate that produced the Communications Decency Act of 1996 (which will dominate our conversation not just today but in the next two classes, as well). The Supreme Court struck down the CDA in *Reno v. ACLU* in 1997, but that didn't stop Congress from trying alternative routes. The readings conclude with a set of problems relating to other federal anti-pornography legislation; try your hand at predicting how these cases ought to come out on the basis of *Reno* and the background briefing.

Preparation questions:

(1) How much pornography is there on the Internet? How easy would it be for a ten-year-old to find it? How likely are they to stumble on it by accident? How effectively could parents prevent that from happening? How easy would it be for a child molester to find the ten-year-old?

(2) Have a look at the *Time* cover accompanying the CDA negotiation problem. The eight-page article accompanying it asked:

> This is the flip side of Vice President Al Gore's vision of an information superhighway linking every school and library in the land. When the kids are plugged in, will they be exposed to the seamiest sides of human sexuality? Will they fall prey to child molesters hanging out in electronic chat rooms?

What's the tone here? How has media coverage of the Internet changed in the last fifteen years? How does the media coverage affect the political debates? Do the mass media still panic over teh interwebs?

(3) Did you catch how the first paragraph of *Reno* refers to "the three-judge District Court?" That's not a misprint. Congress has specified by statute that challenges to the constitutionality of certain federal legislation are to be heard by special three-judge District Courts. In this case, the three judges filed a common introduction and common findings of fact, then each wrote their own conclusions of law. All three agreed that the challenged "indecency" and "harmful-to-minors" provisions of the CDA were unconstitutional. Judge Dalzell's conclusion achieved Internet-wide fame:

> Cutting through the acronyms and argot that littered the hearing testimony, the Internet may fairly be regarded as a never-ending worldwide conversation. The Government may not, through the CDA, interrupt that conversation. As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from governmental intrusion.

> True it is that many find some of the speech on the Internet to be offensive, and amid the din of cyberspace many hear discordant voices that they regard as indecent. The absence of governmental regulation of Internet content has unquestionably produced a kind of chaos, but as one of plaintiffs' experts put it with such resonance at the hearing:
>
> What achieved success was the very chaos that the Internet is. The strength of the Internet is that chaos.
>
> Just as the strength of the Internet is chaos, so the strength of our liberty depends upon the chaos and cacophony of the unfettered speech the First Amendment protects.
>
> For these reasons, I without hesitation hold that the CDA is unconstitutional on its face.

Can you link these phrases back to some of the theorists we've read? Why might this passage have been so inspiring to Internet activists? Keep in mind that this was 1996, and this was the first major legal test the Internet had faced. What might have happened had the decisions in *Reno* gone the other way?

(4) In a famous concurrence in part in *Reno*, Justice O'Connor described the CDA as an attempt to create a "zoning law" for the Internet, dividing it into kid-safe and adults-only zones. Are there kid-safe and adults-only places offline? Would that kind of division be a good thing online, too? Is it harder or easier to zone cyberspace than to zone offline? (Both?) Would it be easier or harder to create kid-safe and adults-only areas online today than it was in 1997?

(5) How many different federal anti-pornography statutes do you count in today's materials? And how many trips to the Supreme Court? Notice a pattern?

Pornography Law primer

Whenever the government tries to restrict access to speech because of its message, rather than how it's communicated, the restriction is said to be *content-based*. Prohibiting "political" speeches in the park is content-based; prohibiting "loud" speeches is content-neutral. A content-based restriction on speech must satisfy a three-pronged "strict scrutiny" test:

(1) There must be a "compelling interest" in restricting access to the speech to be restricted. In practice, this means the speech must be actively harmful in some way and without offsetting benefits. Fraudulent misrepresentation is a good example; it harms the deceived victim, but society doesn't have an interest in the spread of lies.

(2) The restriction must be "narrowly tailored" to the speech it prohibits.

(3) There must be no "less restrictive alternatives" for preventing that speech.

When it comes to pornographic material, the courts have recognized three categories of harmful speech:

Obscenity is material that fails the three-part *Miller* test:

> "(a) whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value."

It can constitutionally be regulated because it has no redeeming social value (see clause (c)) and its offensiveness provides a positive justification for banning it (see clause (b)). The mere possession of obscenity cannot be criminalized, *see Stanley v. Georgia*, 394 U.S. 557 (1969), because doing do would intrude on the privacy of the home, but the government can constitutionally prohibit its distribution and sale.

Child pornography is material that depicts children engaging in sexual acts. It can constitutionally be prohibited outright—that is, it is contraband, and mere possession of it is criminal. (Many child pornography prosecutions, like many drug possession prosecutions, turn on highly factual questions of whether the defendant had sufficient knowledge of or control over the material to "possess" it.) The government has a compelling interest in preventing the exploitation of children in its production. *See New York v. Ferber*, 458 U.S. 747 (1982).

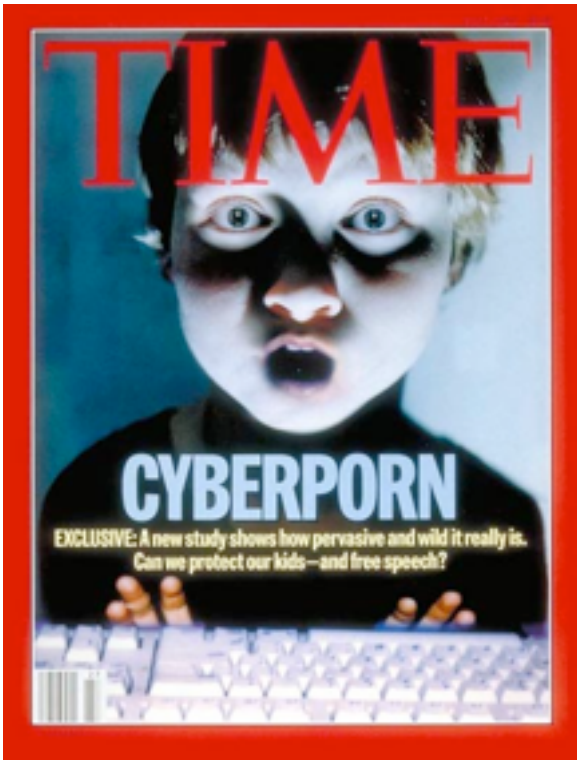
Some material that is legal for adults to possess is nonetheless **harmful to minors**. Thus, for example, the government can prohibit the use of George Carlin's "seven words you can't say on television" on the radio, *see Federal Communications Commission v. Pacifica Foundation*, 438 U.S. 726 (1978) and fine television stations over Janet Jackson's nationally televised, breast-baring "wardrobe malfunction." In both cases, children might be watching, and although it is lawful for adults to receive and exchange such material, the government can pass laws that restrict minors' access to it. The exact contours of this category are subject to debate—one person's "vital sex ed" is another's "vile pornography"—but one thing is clear: the government may *not* ban such material outright or prevent adults from obtaining it, only attempt to restrict minors' access. *Reno v. ACLU* discusses some of the difficulties in drawing these lines.

Note what *isn't* on this list: "pornography." That's not usually a meaningful category for First Amendment purposes. Instead, you typically need to work within one of the above categories—thus, argue that the porn has no redeeming value, that it depicts children, or that it is being shown to minors.

CDA Negotiation Problem

The year is 1995, and the Internet has exploded into public consciousness. Businesses are starting to realize the enormous potential for online commerce and are looking for ways to go online and connect with their customers. Policymakers have also recognized the Internet's huge potential to distribute information; this could be the library and the classroom of the future. But

in the halls of Congress, there is fear, fear that all of this potential could be squandered.



Why? Because of the threat of cyberporn. A study carried out at Carnegie-Mellon published in the *Georgetown Law Journal* surveyed almost a million images, descriptions, stories, and animations, and concluded that over 80% of them were pornographic. *Time* ran a cover story on the study and online threats to children. Now, everyone is talking about the online pornography menace and what to do about it.

In the backrooms of Capitol Hill, key senators have quietly convened a series of conversations about a potential bill to make the Internet safe for average users—and their children. You will represent one of the following groups in an in-class negotiation to work out a legislative compromise.

• **Family Values Coalition**: Religious conservatives, parents' organizations, and anti-pornography liberals dislike pornography in all of its forms, and are especially concerned about the harms it imposes on children. They would like to keep as much pornography as possible off the Internet, and especially want to prevent it from reaching children. They're hopping mad about the Carnegie-Mellon study and want immediate action. They have immense influence, but not enough to pass a bill on their own, without allies.

• **Pornographers**: The adult entertainment industry has little influence in Washington. Whenever they can, however, its lawyers remind Congressional types that the First Amendment protects some forms of pornography. The industry, of course, supports efforts to prevent its wares from reaching children, but will strongly defend, in court if necessary, its right to sell ordinary pornography to willing adults.

• **Civil Libertarians**: The ACLU, American Library Association, and other speech-friendly civil rights groups may not like pornography much, but they will defend anyone's rights to free speech online. They are especially concerned that any attempts to restrict illegal materials not impede people's ability to speak (and receive information) on other subjects—and they also believe that even "obscenity" as currently defined in the law contains some material that ought to be legal. They will fight any legislation that criminalizes distributing legal materials to adults, and are also concerned about anything that restricts people's practical ability to receive such information. They're hopping mad about the Carnegie-Mellon study, which was based on faulty, possibly fraudulent data, but has been uncritically accepted by the media.

• **The Internet Industry**: Companies like AOL and CompuServe provide access to the Internet and forums for discussion and posting information. They aren't in favor of obscenity or child pornography, or in favor of kids seeing porn, and are willing to help out a bit in

restricting access to these materials. But they're strongly opposed to anything that would make them liable for failing to block access to pornography; they already are handling so many messages a day that it would be economically infeasible for them to review each one individually.

• **Congress**: The senators sponsoring this effort are not going to go home without a bill. They would like to take a firm stance to protect children from the dangers of pornography, and to pave the way for safe commerce on the Internet. They're sensitive to coalitions; they don't want anyone so upset at the legislative result that campaign donations start flowing to their challengers. Whatever passes should hold up in court, if possible.

Can you think of provisions and compromises that might satisfy all—or most—of these constituencies? What will your negotiating position be, and what should the final bill look like? Keep in mind that perfect agreement on all issues may not be possible, and that legislation can sometimes defer tough issues for later resolution (how?). Remember also that the technological savviness of these groups varies enormously. And, of course, don't forget that the question of whether ISPs and other internet intermediaries should be liable for pornographic content on their systems was also on the table.

Reno v. ACLU
521 US 844 (1997)

Justice Stevens delivered the opinion of the Court.

At issue is the constitutionality of two statutory provisions enacted to protect minors from "indecent" and "patently offensive" communications on the Internet. Notwithstanding the legitimacy and importance of the congressional goal of protecting children from harmful materials, we agree with the three-judge District Court that the statute abridges "the freedom of speech" protected by the First Amendment.

II

The first, 47 U. S. C. § 223(a) (1994 ed., Supp. II), prohibits the knowing transmission of obscene or indecent messages to any recipient under 18 years of age. It provides in pertinent part:

"(a) Whoever—

"(1) in interstate or foreign communications—

. . . . .

"(B) by means of a telecommunications device knowingly—

"(i) makes, creates, or solicits, and

"(ii) initiates the transmission of, "any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication;

. . . . .

"(2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity, "shall be fined under Title 18, or imprisoned not more than two years, or both."

The second provision, § 223(d), prohibits the knowing sending or displaying of patently offensive messages in a manner that is available to a person under 18 years of age. It provides:

"(d) Whoever—

"(1) in interstate or foreign communications knowingly—

"(A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or

"(B) uses any interactive computer service to display in a manner available to a person under 18 years of age, "any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or

"(2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity, "shall be fined under Title 18, or imprisoned not more than two years, or both."

The breadth of these prohibitions is qualified by two affirmative defenses. See § 223(e)(5). One covers those who take "good faith, reasonable, effective, and appropriate actions" to restrict access by minors to the prohibited communications. § 223(e)(5)(A). The other covers those who restrict access to covered material by requiring certain designated forms of age proof, such as a verified credit card or an adult identification number or code. § 223(e)(5)(B). ...

VI

The Government argues that the statute is no more vague than the obscenity standard this Court established in *Miller v. California, 413 U. S. 15 (1973)*. But that is not so. In *Miller,* this Court reviewed a criminal conviction against a commercial vendor who mailed brochures containing pictures of sexually explicit activities to individuals who had not requested such materials. *Id.,* at 18. Having struggled for some time to establish a definition of obscenity, we set forth in *Miller* the test for obscenity that controls to this day:

"(a) whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value." *Id.,* at 24 (internal quotation marks and citations omitted).

Because the CDA's "patently offensive" standard (and, we assume, *arguendo,* its synonymous "indecent" standard) is one part of the three-prong *Miller* test, the Government reasons, it cannot be unconstitutionally vague. ...

Just because a definition including three limitations is not vague, it does not follow that one of those limitations, standing by itself, is not vague.Each of *Miller* `s additional two prongs—(1) that, taken as a whole, the material appeal to the "prurient" interest, and (2) that it "lac[k] serious literary, artistic, political, or scientific value"—critically limits the uncertain sweep of the obscenity definition. The second requirement is particularly important because, unlike the "patently offensive" and "prurient interest" criteria, it is not judged by contemporary community standards. See *Pope v. Illinois, 481 U. S. 497, 500 (1987)*. This "societal value" requirement, absent in the CDA, allows appellate courts to impose some limitations and regularity on the definition by setting, as a matter of law, a national floor for socially redeeming value. The Government's contention that courts will be able to give such legal limitations to the CDA's standards is belied by *Miller* `s own rationale for having juries determine whether material is "patently offensive" according to community standards: that such questions are essentially ones of *fact*.

In contrast to *Miller* and our other previous cases, the CDA thus presents a greater threat of censoring speech that, in fact, falls outside the statute's scope. Given the vague contours of the coverage of the statute, it unquestionably silences some speakers whose messages would be entitled to constitutional protection. That danger provides further reason for insisting that the statute not be overly broad. The CDA's burden on protected speech cannot be justified if it could be avoided by a more carefully drafted statute.

VII

We are persuaded that the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech. In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another. That burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.

In evaluating the free speech rights of adults, we have made it perfectly clear that "[s]exual expression which is indecent but not obscene is protected by the First Amendment." *Sable, 492 U. S., at 126*. See also *Carey v. Population Services Int'l, 431 U. S. 678, 701 (1977)* ("[W]here obscenity is not involved, we have consistently held that the 875 fact that protected speech may be offensive to some does not justify its suppression"). Indeed, *Pacifica* itself admonished that "the fact that society may find speech offensive is not a sufficient reason for suppressing it." 438 U. S., at 745.

It is true that we have repeatedly recognized the governmental interest in protecting children from harmful materials. See *Ginsberg, 390 U. S., at 639*; *Pacifica, 438 U. S., at 749*. But that interest does not justify an unnecessarily broad suppression of speech addressed to adults. As we have explained, the Government may not "reduc[e] the adult population . . . to . . . only what is fit for children." *Denver, 518 U. S., at 759* (internal quotation marks omitted) (quoting *Sable, 492 U. S., at 128*). "[R]egardless of the strength of the government's interest" in protecting children, "[t]he level of discourse reaching a mailbox simply cannot be limited to that which would be suitable for a sandbox." *Bolger v. Youngs Drug Products Corp., 463 U. S. 60, 74-75 (1983)*.

The District Court was correct to conclude that the CDA effectively resembles the ban on "dial-a-porn" invalidated in *Sable*. 929 F. Supp., at 854. In *Sable, 492 U. S., at 129*, this Court rejected the argument that we should defer to the congressional judgment that nothing less than a total ban would be effective in preventing enterprising youngsters from gaining access to indecent

communications. *Sable* thus made clear that the mere fact that a statutory regulation of speech was enacted for the important purpose of protecting children from exposure to sexually explicit material does not foreclose inquiry into its validity. As we pointed out last Term, that inquiry embodies an "overarching commitment" to make sure that Congress has designed its statute to accomplish its purpose "without imposing an unnecessarily great restriction on speech." *Denver, 518 U. S., at 741.*

In arguing that the CDA does not so diminish adult communication, the Government relies on the incorrect factual premise that prohibiting a transmission whenever it is known that one of its recipients is a minor would not interfere with adult-to-adult communication. The findings of the District Court make clear that this premise is untenable. Given the size of the potential audience for most messages, in the absence of a viable age verification process, the sender must be charged with knowing that one or more minors will likely view it. Knowledge that, for instance, one or more members of a 100-person chat group will be a minor—and therefore that it would be a crime to send the group an indecent message—would surely burden communication among adults.

The District Court found that at the time of trial existing technology did not include any effective method for a sender to prevent minors from obtaining access to its communications on the Internet without also denying access to adults. The Court found no effective way to determine the age of a user who is accessing material through e-mail, mail exploders, newsgroups, or chat rooms. 929 F. Supp., at 845. As a practical matter, the Court also found that it would be prohibitively expensive for noncommercial— as well as some commercial—speakers who have Web sites to verify that their users are adults. *Id.,* at 845-848 . These limitations must inevitably curtail a significant amount of adult communication on the Internet. By contrast, the District Court found that "[d]espite its limitations, currently available *user-based* software suggests that a reasonably effective method by which *parents* can prevent their children from accessing sexually explicit and other material which *parents* may believe is inappropriate for their children will soon be widely available." *Id.*, at 842 ((emphases added).

The breadth of the CDA's coverage is wholly unprecedented. Unlike the regulations upheld in *Ginsberg* and *Pacifica,* the scope of the CDA is not limited to commercial speech or commercial entities. Its open-ended prohibitions embrace all nonprofit entities and individuals posting indecent messages or displaying them on their own computers in the presence of minors. The general, undefined terms "indecent" and "patently offensive" cover large amounts of nonpornographic material with serious educational or other value. Moreover, the "community standards" criterion as applied to the Internet means that any communication available to a nationwide audience will be judged by the standards of the community most likely to be offended by the message. The regulated subject matter includes any of the seven "dirty words" used in the *Pacifica* monologue, the use of which the Government's expert acknowledged could constitute a felony. It may also extend to discussions about prison rape or safe sexual practices, artistic images that include nude subjects, and arguably the card catalog of the Carnegie Library.

For the purposes of our decision, we need neither accept nor reject the Government's submission that the First Amendment does not forbid a blanket prohibition on all "indecent" and "patently offensive" messages communicated to a 17-year-old—no matter how much value the message may contain and regardless of parental approval. It is at least clear that the strength of the Government's interest in protecting minors is not equally strong throughout the coverage of

this broad statute. Under the CDA, a parent allowing her 17-year-old to use the family computer to obtain information on the Internet that she, in her parental judgment, deems appropriate could face a lengthy prison term. See 47 U. S. C. § 223(a)(2) (1994 ed., Supp. II). Similarly, a parent who sent his 17-year-old college freshman information on birth control via e-mail could be incarcerated even though neither he, his child, nor anyone in their home community found the material "indecent" or "patently offensive," if the college town's community thought otherwise.

The breadth of this content-based restriction of speech imposes an especially heavy burden on the Government to explain why a less restrictive provision would not be as effective as the CDA. It has not done so. The arguments in this Court have referred to possible alternatives such as requiring that indecent material be "tagged" in a way that facilitates parental control of material coming into their homes, making exceptions for messages with artistic or educational value, providing some tolerance for parental choice, and regulating some portions of the Internet —such as commercial Web sites—differently from others, such as chat rooms. Particularly in the light of the absence of any detailed findings by the Congress, or even hearings addressing the special problems of the CDA, we are persuaded that the CDA is not narrowly tailored if that requirement has any meaning at all.

VIII

... The Government also asserts that the "knowledge" requirement of both §§ 223(a) and (d), especially when coupled with the "specific child" element found in § 223(d), saves the CDA from overbreadth. Because both sections prohibit the dissemination of indecent messages only to persons known to be under 18, the Government argues, it does not require transmitters to "refrain from communicating indecent material to adults; they need only refrain from disseminating such materials to persons they know to be under 18." Brief for Appellants 24. This argument ignores the fact that most Internet forums—including chat rooms, newsgroups, mail exploders, and the Web—are open to all comers. The Government's assertion that the knowledge requirement somehow protects the communications of adults is therefore untenable. Even the strongest reading of the "specific person" requirement of § 223(d) cannot save the statute. It would confer broad powers of censorship, in the form of a "heckler's veto," upon any opponent of indecent speech who might simply log on and inform the would-be discoursers that his 17-year-old child—a "specific person . . . under 18 years of age," 47 U. S. C. § 223(d)(1)(A) (1994 ed., Supp. II)—would be present.

IX

The Government's three remaining arguments focus on the defenses provided in § 223(e)(5).First, relying on the "good faith, reasonable, effective, and appropriate actions" provision, the Government suggests that "tagging" provides a defense that saves the constitutionality of the CDA. The suggestion assumes that transmitters may encode their indecent communications in a way that would indicate their contents, thus permitting recipients to block their reception with appropriate software. It is the requirement that the good-faith action must be "effective" that makes this defense illusory. The Government recognizes that its proposed screening software does not currently exist. Even if it did, there is no way to know whether a potential recipient will actually block the encoded material. Without the impossible knowledge that every guardian in America is screening for the "tag," the transmitter could not reasonably rely on its action to be "effective."

For its second and third arguments concerning defenses— which we can consider together —the Government relies on the latter half of § 223(e)(5), which applies when the transmitter has restricted access by requiring use of a verified credit card or adult identification. Such verification is not only technologically available but actually is used by commercial providers of sexually explicit material. These providers, therefore, would be protected by the defense. Under the findings of the District Court, however, it is not economically feasible for most noncommercial speakers to employ such verification. Accordingly, this defense would not significantly narrow the statute's burden on noncommercial speech. Even with respect to the commercial pornographers that would be protected by the defense, the Government failed to adduce any evidence that these verification techniques actually preclude minors from posing as adults.Given that the risk of criminal sanctions "hovers over each content provider, like the proverbial sword of Damocles," 929 F. Supp., at 855-856. the District Court correctly refused to rely on unproven future technology to save the statute. The Government thus failed to prove that the proffered defense would significantly reduce the heavy burden on adult speech produced by the prohibition on offensive displays.

We agree with the District Court's conclusion that the CDA places an unacceptably heavy burden on protected speech, and that the defenses do not constitute the sort of "narrow tailoring" that will save an otherwise patently invalid unconstitutional provision. In *Sable, 492 U. S., at 127,* we remarked that the speech restriction at issue there amounted to "`burn[ing] the house to roast the pig.' " The CDA, casting a far darker shadow over free speech, threatens to torch a large segment of the Internet community.

Pornography Law Problems

(1) The federal Child Pornography Protection Act (CPPA) of 1996 prohibits the distribution of "any visual depiction, including any photograph, film, video, picture, or computer or computer- generated image or picture" that "is, or appears to be, of a minor engaging in sexually explicit conduct." A group of artists and free speech activists have argued that the statute is unconstitutional because it would prohibit purely computer-generated images, or movies produced using actors who appear younger than they are. *See Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002); *Cf. United States v. Williams*, 553 U.S. 285 (2008).

(2) The obscenity provisions of the federal Communications Decency Act of 1996 prohibits "by means of a telecommunications device knowingly . . . initiat[ing] the transmission of[] any comment, request, suggestion, proposal, image, or other communication which is obscene or child pornography, knowing that the recipient of the communication is under 18 years of age." An artist who creates works with sexual sadomasochistic themes and a not-for-profit organization promoting polyamory challenge the statute. They argue that statute inappropriately applies the *Miller* definition of "obscene" to the Internet, because the "contemporary community standards" (prong (a)) and the consensus of what is "patently offensive" (prong (b)) could be drawn from any community in the United States. *See Nitke v. Gonzales*, 413 F. Supp. 2d 262 (2005); *cf. Ashcroft v. ACLU,* 535 U.S. 564 (2002) (considering challenge on similar grounds to federal Child Online Protection Act (COPA) of 1998).

(3) The federal Child Protection and Obscenity Enforcement Act of 1988 (CPOEA) requires that those who create materials depicting "actual sexually explicit conduct" must

maintain records of each performer or model's photo identification proving that they are not minors. This statute has survived various constitutional challenges, in part because its definition of "actual sexually explicit conduct" has been held to be both narrow and precise. A more recent amendment, the federal Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today (PROTECT) Act, of 2003 extends this requirement to include digital and computer-manipulated images and videos, and requires those who upload such materials onto websites to maintain the same records. The Free Speech Coalition, an adult entertainment industry trade association, challenges the amendment as imposing an insurmountable burden on website maintainers, who may be distributing many thousands of images or videos. *See, e.g. Free Speech Coalition v. Gonzales*, 406 F. .Supp. 2d 1196 (D. Colo. 2005)

(4) The federal Child Online Protection Act (COPA) of 1998 prohibits "knowingly" making any material available on the Web to a minor that contains any material that is "harmful to minors." The statute contains a definition of "harmful to minors" that tracks the *Ferber* definitions, but tack on the words "with respect to minors" to each prong. The ACLU sues. It argues that the law is inappropriate because the prohibition isn't narrowly tailored and because filtering software—which limits the websites a computer can access—installed on children's' computers by their guardians would be a less restrictive alternative. *See Ashcroft v. ACLU*, 542 US 656 (2004), *on remand at ACLU v. Gonzales*, 478 F. Supp. 2d 775 (E.D. Pa. 2007).

(5) Contrariwise, the federal Children's Internet Protection Act (CIPA) of 2000 applies to libraries and schools that receive federal subsidies for purchasing Internet access or computers. They must equip computers on which they supply Internet access with filters that block access to "visual depictions" that are obscene or constitute child pornography, and that prevent minors from accessing "visual depictions" that are "harmful to minors." The American Library Association sues to block implementation of CIPA, arguing that all existing filtering software overblocks a great deal of material that is not obscene or harmful to minors, and that while libraries are permitted to disable the filters upon request by an adult patron, they are not required to do so. *See United States v. American Library Association*, 539 U.S. 194 (2003).

CLASS 10: SECTION 230

Last time, we saw that the CDA was a result of legislative compromise. The price that the Internet companies demanded as part of their cooperation was embodied in Section 230 of the Telecommunications Act, which was codified at 47 U.S.C. § 230. It's since become known as "Section 230," and it is, bar none, the single most important piece of law you will learn in this course. The basic idea of § 230 is simple: if I post a defamatory video to YouTube, I'm the one who should be held liable for it, not YouTube. But, as we will see, the exact scope of this immunity was up for grabs in the first few years. The courts have chosen to interpret it broadly —creating a kind of immunity with no parallel in law offline. Today's readings are focused on the landmark case of *Zeran v. AOL* and its aftermath.

Starting with today, and continuing for the next few weeks, our cases heavily explore the course's third major theme: intermediary power. Intermediary immunity is a policy choice, one that increases the effective flexibility and power of the intermediaries it protects. As you prepare for these classes, ask yourself what goals that immunity is meant to serve, and who else benefits (or loses) when intermediaries are empowered in this way.

Preparation questions:

(1) I cannot overstate how important Section 230 is. It will be on the final. If I had to pick one thing in this course that I wish every student graduating from law school knew, I'd pick Section 230. As construed by the courts, it's (a) relevant in a wide range of cases, (b) clear and easy to understand, and (c) very surprising. Get familiar with it. Now state the rule of Section 230, post-*Zeran*, in your own words, in one sentence.

(2) Section 230 was part of the legislative deal that produced the Communications Decency Act. How does an immunity for ISPs and other online intermediaries fit with a law punishing putting indecent material online? Why did the Internet companies ask for it? Why were the other parties in the negotiations willing to grant it to them? Given that the indecency and harmful-to-minors pieces of the CDA were ruled unconstitutional in short order, who's laughing now? Does the scope of the immunity post-*Zeran* and post-*Drudge* correspond to what, say, the anti-porn crusaders thought they were giving the Internet companies? Is there anything ironic about this outcome?

(3) Explain the distinction between "publisher" and "distributor" liability at common law. Explain *Zeran's* holding in terms of these categories. Now explain it again, slowly. Now test yourself: After *Zeran*, if you find a defamatory post about you on AOL, can you sue AOL? What if you pick up the phone and call AOL and tell them, "There's a defamatory post about me!" Your answers should be "no" and "no." Explain why.

(4) There were three potential defendants in *Zeran*: Ken ZZ03, AOL, and KRXO. Ken Zeran recovered nothing from any of them. He couldn't sue KRXO because they didn't harm his reputation with anyone who actually knew him; *Zeran* holds that he couldn't sue AOL; why couldn't he sue Ken ZZ03? How about Sidney Blumenthal's suit against Matt Drudge; would that one succeed?

(5) *Drudge* extends *Zeran*. How? How is what AOL did to Sidney Blumenthal worse than what it did to Ken Zeran? Why do opponents of Section 230 say that its effects are toxic in giving intermediaries no incentives whatsoever to be responsible Internet citizens? How

would proponents of Section 230 respond? Look at the *Zeran* court's discussion of the incentives produced by the *Stratton Oakmont* decision. Are you convinced? Why or why not?

(6) How would AOL have to change the way it does business if it were held liable as a distributor? If it were held liable as a publisher? What about YouTube, to which users upload hundreds of thousands of videos daily? Fans of Section 230 believe that it's been responsible for the explosive growth of user-generated content sites in the decade-plus since it was enacted. What does these things have to do with each other? What do you think of this policy argument for the result in *Zeran*?

47 U.S.C. § 230 (excerpt)

§ 230. Protection for private blocking and screening of offensive material

...

(c) Protection for "Good Samaritan" blocking and screening of offensive material

(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).

Zeran v. America Online, Inc.
129 F.3d 327 (1997)

WILKINSON, Chief Judge:

Kenneth Zeran brought this action against America Online, Inc. ("AOL"), arguing that AOL unreasonably delayed in removing defamatory messages posted by an unidentified third party, refused to post retractions of those messages, and failed to screen for similar postings thereafter. The district court granted judgment for AOL on the grounds that the Communications Decency Act of 1996 ("CDA") — 47 U.S.C. § 230 — bars Zeran's claims. Zeran appeals, arguing that § 230 leaves intact liability for interactive computer service providers who possess notice of defamatory material posted through their services. He also contends that § 230 does not apply here because his claims arise from AOL's alleged negligence prior to the

CDA's enactment. Section 230, however, plainly immunizes computer service providers like AOL from liability for information that originates with third parties. Furthermore, Congress clearly expressed its intent that § 230 apply to lawsuits, like Zeran's, instituted after the CDA's enactment. Accordingly, we affirm the judgment of the district court.

I.

"The Internet is an international network of interconnected computers," currently used by approximately 40 million people worldwide. Reno v. ACLU, ___ U.S. ___, ___, 117 S.Ct. 2329, 2334, 138 L.Ed.2d 874 (1997). One of the many means by which individuals access the Internet is through an interactive computer service. These services offer not only a connection to the Internet as a whole, but also allow their subscribers to access information communicated and stored only on each computer service's individual proprietary network. Id. AOL is just such an interactive computer service. Much of the information transmitted over its network originates with the company's millions of subscribers. They may transmit information privately via electronic mail, or they may communicate publicly by posting messages on AOL bulletin boards, where the messages may be read by any AOL subscriber.

The instant case comes before us on a motion for judgment on the pleadings, see Fed.R.Civ.P. 12(c), so we accept the facts alleged in the complaint as true. Bruce v. Riddle, 631 F. 2d 272, 273 (4th Cir.1980). On April 25, 1995, an unidentified person posted a message on an AOL bulletin board advertising "Naughty Oklahoma T-Shirts." The posting described the sale of shirts featuring offensive and tasteless slogans related to the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City. Those interested in purchasing the shirts were instructed to call "Ken" at Zeran's home phone number in Seattle, Washington. As a result of this anonymously perpetrated prank, Zeran received a high volume of calls, comprised primarily of angry and derogatory messages, but also including death threats. Zeran could not change his phone number because he relied on its availability to the public in running his business out of his home. Later that day, Zeran called AOL and informed a company representative of his predicament. The employee assured Zeran that the posting would be removed from AOL's bulletin board but explained that as a matter of policy AOL would not post a retraction. The parties dispute the date that AOL removed this original posting from its bulletin board.

On April 26, the next day, an unknown person posted another message advertising additional shirts with new tasteless slogans related to the Oklahoma City bombing. Again, interested buyers were told to call Zeran's phone number, to ask for "Ken," and to "please call back if busy" due to high demand. The angry, threatening phone calls intensified. Over the next four days, an unidentified party continued to post messages on AOL's bulletin board, advertising additional items including bumper stickers and key chains with still more offensive slogans. During this time period, Zeran called AOL repeatedly and was told by company representatives that the individual account from which the messages were posted would soon be closed. Zeran also reported his case to Seattle FBI agents. By April 30, Zeran was receiving an abusive phone call approximately every two minutes.

Meanwhile, an announcer for Oklahoma City radio station KRXO received a copy of the first AOL posting. On May 1, the announcer related the message's contents on the air, attributed them to "Ken" at Zeran's phone number, and urged the listening audience to call the number. After this radio broadcast, Zeran was inundated with death threats and other violent calls from

Oklahoma City residents. Over the next few days, Zeran talked to both KRXO and AOL representatives. He also spoke to his local police, who subsequently surveilled his home to protect his safety. By May 14, after an Oklahoma City newspaper published a story exposing the shirt advertisements as a hoax and after KRXO made an on-air apology, the number of calls to Zeran's residence finally subsided to fifteen per day.

Zeran first filed suit on January 4, 1996, against radio station KRXO in the United States District Court for the Western District of Oklahoma. On April 23, 1996, he filed this separate suit against AOL in the same court. Zeran did not bring any action against the party who posted the offensive messages. After Zeran's suit against AOL was transferred to the Eastern District of Virginia pursuant to 28 U.S.C. § 1404(a), AOL answered Zeran's complaint and interposed 47 U.S.C. § 230 as an affirmative defense. AOL then moved for judgment on the pleadings pursuant to Fed.R.Civ.P. 12(c). The district court granted AOL's motion, and Zeran filed this appeal.

II.

A.

Because § 230 was successfully advanced by AOL in the district court as a defense to Zeran's claims, we shall briefly examine its operation here. Zeran seeks to hold AOL liable for defamatory speech initiated by a third party. He argued to the district court that once he notified AOL of the unidentified third party's hoax, AOL had a duty to remove the defamatory posting promptly, to notify its subscribers of the message's false nature, and to effectively screen future defamatory material. Section 230 entered this litigation as an affirmative defense pled by AOL. The company claimed that Congress immunized interactive computer service providers from claims based on information posted by a third party.

The relevant portion of § 230 states: "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." 47 U.S.C. § 230(c)(1). 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. Specifically, § 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions — such as deciding whether to publish, withdraw, postpone or alter content — are barred.

The purpose of this statutory immunity is not difficult to discern. Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum. In specific statutory findings, Congress recognized the Internet and interactive computer services as offering "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity." Id. § 230(a)(3). It also found that the Internet and interactive computer services "have flourished, to the benefit of all Americans, with a minimum of government regulation." Id. § 230(a)(4) (emphasis added). Congress further stated that it is "the policy of the United States ... 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." Id. § 230(b)(2) (emphasis added).

None of this means, of course, that the original culpable party who posts defamatory messages would escape accountability. While Congress acted to keep government regulation of the Internet to a minimum, it also found it to be the policy of the United States "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer." Id. § 230(b)(5). Congress made a policy choice, however, not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages.

Congress' purpose in providing the § 230 immunity was thus evident. Interactive computer services have millions of users. See Reno v. ACLU, ___ U.S. at ___, 117 S.Ct. at 2334 (noting that at time of district court trial, "commercial online services had almost 12 million individual subscribers"). The amount of information communicated via interactive computer services is therefore staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect.

Another important purpose of § 230 was to encourage service providers to self-regulate the dissemination of offensive material over their services. In this respect, § 230 responded to a New York state court decision, Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y.Sup.Ct. May 24, 1995). There, the plaintiffs sued Prodigy — an interactive computer service like AOL — for defamatory comments made by an unidentified party on one of Prodigy's bulletin boards. The court held Prodigy to the strict liability standard normally applied to original publishers of defamatory statements, rejecting Prodigy's claims that it should be held only to the lower "knowledge" standard usually reserved for distributors. The court reasoned that Prodigy acted more like an original publisher than a distributor both because it advertised its practice of controlling content on its service and because it actively screened and edited messages posted on its bulletin boards.

Congress enacted § 230 to remove the disincentives to selfregulation created by the Stratton Oakmont decision. Under that court's holding, computer service providers who regulated the dissemination of offensive material on their services risked subjecting themselves to liability, because such regulation cast the service provider in the role of a publisher. Fearing that the specter of liability would therefore deter service providers from blocking and screening offensive material, Congress enacted § 230's broad immunity "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." 47 U.S.C. § 230(b)(4). In line with this purpose, § 230 forbids the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions.

B.

Zeran argues, however, that the § 230 immunity eliminates only publisher liability, leaving distributor liability intact. Publishers can be held liable for defamatory statements contained in

their works even absent proof that they had specific knowledge of the statement's inclusion. W. Page Keeton et al., Prosser and Keeton on the Law of Torts § 113, at 810 (5th ed.1984). According to Zeran, interactive computer service providers like AOL are normally considered instead to be distributors, like traditional news vendors or book sellers. Distributors cannot be held liable for defamatory statements contained in the materials they distribute unless it is proven at a minimum that they have actual knowledge of the defamatory statements upon which liability is predicated. Id. at 811 (explaining that distributors are not liable "in the absence of proof that they knew or had reason to know of the existence of defamatory matter contained in matter published"). Zeran contends that he provided AOL with sufficient notice of the defamatory statements appearing on the company's bulletin board. This notice is significant, says Zeran, because AOL could be held liable as a distributor only if it acquired knowledge of the defamatory statements' existence.

Because of the difference between these two forms of liability, Zeran contends that the term "distributor" carries a legally distinct meaning from the term "publisher." Accordingly, he asserts that Congress' use of only the term "publisher" in § 230 indicates a purpose to immunize service providers only from publisher liability. He argues that distributors are left unprotected by § 230 and, therefore, his suit should be permitted to proceed against AOL. We disagree. Assuming arguendo that Zeran has satisfied the requirements for imposition of distributor liability, this theory of liability is merely a subset, or a species, of publisher liability, and is therefore also foreclosed by § 230.

The terms "publisher" and "distributor" derive their legal significance from the context of defamation law. Although Zeran attempts to artfully plead his claims as ones of negligence, they are indistinguishable from a garden variety defamation action. Because the publication of a statement is a necessary element in a defamation action, only one who publishes can be subject to this form of tort liability. Restatement (Second) of Torts § 558(b) (1977); Keeton et al., supra, § 113, at 802. Publication does not only describe the choice by an author to include certain information. In addition, both the negligent communication of a defamatory statement and the failure to remove such a statement when first communicated by another party— each alleged by Zeran here under a negligence label—constitute publication. Restatement (Second) of Torts § 577; see also Tacket v. General Motors Corp., 836 F.2d 1042, 1046-47 (7th Cir.1987). In fact, every repetition of a defamatory statement is considered a publication. Keeton et al., supra, § 113, at 799.

In this case, AOL is legally considered to be a publisher. "[E]very one who takes part in the publication ... is charged with publication." Id. Even distributors are considered to be publishers for purposes of defamation law:

> Those who are in the business of making their facilities available to disseminate the writings composed, the speeches made, and the information gathered by others may also be regarded as participating to such an extent in making the books, newspapers, magazines, and information available to others as to be regarded as publishers. They are intentionally making the contents available to others, sometimes without knowing all of the contents—including the defamatory content — and sometimes without any opportunity to ascertain, in advance, that any defamatory matter was to be included in the matter published.

Id. at 803. AOL falls squarely within this traditional definition of a publisher and, therefore, is clearly protected by § 230's immunity.

Zeran contends that decisions like Stratton Oakmont and Cubby, Inc. v. CompuServe Inc., 776 F.Supp. 135 (S.D.N.Y.1991), recognize a legal distinction between publishers and distributors. He misapprehends, however, the significance of that distinction for the legal issue we consider here. It is undoubtedly true that mere conduits, or distributors, are subject to a different standard of liability. As explained above, distributors must at a minimum have knowledge of the existence of a defamatory statement as a prerequisite to liability. But this distinction signifies only that different standards of liability may be applied within the larger publisher category, depending on the specific type of publisher concerned. See Keeton et al., supra, § 113, at 799-800 (explaining that every party involved is charged with publication, although degrees of legal responsibility differ). To the extent that decisions like Stratton and Cubby utilize the terms "publisher" and "distributor" separately, the decisions correctly describe two different standards of liability. Stratton and Cubby do not, however, suggest that distributors are not also a type of publisher for purposes of defamation law.

Zeran simply attaches too much importance to the presence of the distinct notice element in distributor liability. The simple fact of notice surely cannot transform one from an original publisher to a distributor in the eyes of the law. To the contrary, once a computer service provider receives notice of a potentially defamatory posting, it is thrust into the role of a traditional publisher. The computer service provider must decide whether to publish, edit, or withdraw the posting. In this respect, Zeran seeks to impose liability on AOL for assuming the role for which § 230 specifically proscribes liability — the publisher role.

Our view that Zeran's complaint treats AOL as a publisher is reinforced because AOL is cast in the same position as the party who originally posted the offensive messages. According to Zeran's logic, AOL is legally at fault because it communicated to third parties an allegedly defamatory statement. This is precisely the theory under which the original poster of the offensive messages would be found liable. If the original party is considered a publisher of the offensive messages, Zeran certainly cannot attach liability to AOL under the same theory without conceding that AOL too must be treated as a publisher of the statements.

Zeran next contends that interpreting § 230 to impose liability on service providers with knowledge of defamatory content on their services is consistent with the statutory purposes outlined in Part IIA. Zeran fails, however, to understand the practical implications of notice liability in the interactive computer service context. Liability upon notice would defeat the dual purposes advanced by § 230 of the CDA. Like the strict liability imposed by the Stratton Oakmont court, liability upon notice reinforces service providers' incentives to restrict speech and abstain from self-regulation.

If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement — from any party, concerning any message. Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information. Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context. Cf. Auvil v. CBS 60 Minutes, 800 F.Supp.

928, 931 (E.D.Wash.1992) (recognizing that it is unrealistic for network affiliates to "monitor incoming transmissions and exercise on-the-spot discretionary calls"). Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages upon notification, whether the contents were defamatory or not. See Philadelphia Newspapers, Inc. v. Hepps, 475 U.S. 767, 777, 106 S.Ct. 1558, 1564, 89 L.Ed.2d 783 (1986) (recognizing that fears of unjustified liability produce a chilling effect antithetical to First Amendment's protection of speech). Thus, like strict liability, liability upon notice has a chilling effect on the freedom of Internet speech.

Similarly, notice-based liability would deter service providers from regulating the dissemination of offensive material over their own services. Any efforts by a service provider to investigate and screen material posted on its service would only lead to notice of potentially defamatory material more frequently and thereby create a stronger basis for liability. Instead of subjecting themselves to further possible lawsuits, service providers would likely eschew any attempts at selfregulation.

More generally, notice-based liability for interactive computer service providers would provide third parties with a no-cost means to create the basis for future lawsuits. Whenever one was displeased with the speech of another party conducted over an interactive computer service, the offended party could simply "notify" the relevant service provider, claiming the information to be legally defamatory. In light of the vast amount of speech communicated through interactive computer services, these notices could produce an impossible burden for service providers, who would be faced with ceaseless choices of suppressing controversial speech or sustaining prohibitive liability. Because the probable effects of distributor liability on the vigor of Internet speech and on service provider selfregulation are directly contrary to § 230's statutory purposes, we will not assume that Congress intended to leave liability upon notice intact. . . .

Blumenthal v. Drudge
992 F. Supp. 44 (D.D.C. 1998)

PAUL L. FRIEDMAN, District Judge.

This is a defamation case revolving around a statement published on the Internet by defendant Matt Drudge. On August 10, 1997, the following was available to all having access to the Internet:

> The DRUDGE REPORT has learned that top GOP operatives who feel there is a double-standard of only reporting republican shame believe they are holding an ace card: New White House recruit Sidney Blumenthal has a spousal abuse past that has been effectively covered up.
>
> The accusations are explosive.
>
> There are court records of Blumenthal's violence against his wife, one influential republican, who demanded anonymity, tells the DRUDGE REPORT.
>
> If they begin to use [Don] Sipple and his problems against us, against the Republican Party ... to show hypocrisy, Blumenthal would become fair game. Wasn't it Clinton who signed the Violence Against Women Act?

> [There goes the budget deal honeymoon.] One White House source, also requesting anonymity, says the Blumenthal wife-beating allegation is a pure fiction that has been created by Clinton enemies. [The First Lady] would not have brought him in if he had this in his background, assures the wellplaced staffer. This story about Blumenthal has been in circulation for years.
>
> Last month President Clinton named Sidney Blumenthal an Assistant to the President as part of the Communications Team. He's brought in to work on communications strategy, special projects themeing — a newly created position.
>
> Every attempt to reach Blumenthal proved unsuccessful.

Currently before this Court are a motion for summary judgment filed by defendant America Online, Inc. ("AOL") and a motion to dismiss or transfer for lack of personal jurisdiction filed by defendant Matt Drudge. Upon consideration of the papers filed by the parties and the oral arguments of counsel, the Court concludes that AOL's motion should be granted and Drudge's motion should be denied.

I. BACKGROUND

Plaintiffs Sidney Blumenthal and Jacqueline Jordan Blumenthal are citizens of the District of Columbia and have continuously lived in the District since 1985. Sidney Blumenthal works in the White House as an Assistant to the President of the United States. His first day of work as Assistant to the President was Monday, August 11, 1997, the day after the publication of the alleged defamatory statement. Jacqueline Jordan Blumenthal, Sidney Blumenthal's wife, also works in the White House as Director of the President's Commission On White House Fellowships.

Defendant Matt Drudge, a Takoma Park, Maryland native, is a resident of the State of California, where he has lived continuously since 1987. In early 1995, defendant Drudge created an electronic publication called the Drudge Report, a gossip column focusing on gossip from Hollywood and Washington, D.C. Mr. Drudge's base of operations for writing, publishing and disseminating the Drudge Report has been an office in his apartment in Los Angeles, California.

Access to defendant Drudge's world wide web site is available at no cost to anyone who has access to the Internet at the Internet address of "www.drudgereport.com." The front page of the web site contains the logo "Drudge Report." Defendant Drudge has also placed a hyperlink on his web site that, when activated, causes the most recently published edition of the Drudge Report to be displayed. The web site also contains numerous hyperlinks to other on-line news publications and news articles that may be of interest to readers of the Drudge Report. Id. In addition, during the time period relevant to this case, Drudge had developed a list of regular readers or subscribers to whom he e-mailed each new edition of the Drudge Report. By March 1995, the Drudge Report had 1,000 e-mail subscribers, and plaintiffs allege that by 1997 Drudge had 85,000 subscribers to his e-mail service.

In late 1996, defendant Drudge entered into a six-month licensing agreement with the publisher of "Wired" magazine. Under the agreement, the publisher of "Wired" had the right to receive and display future editions of the Drudge Report in "Hotwired," a new electronic Internet publication. In exchange, defendant Drudge received a bi-weekly royalty payment. In

addition to the publication of the Drudge Report in "Hotwired," defendant Drudge continued to distribute each new edition via e-mail to his subscribers and via his world wide web site.

In late May or early June of 1997, at approximately the time when the "Wired" licensing agreement expired, defendant Drudge entered into a written license agreement with AOL. The agreement made the Drudge Report available to all members of AOL's service for a period of one year. In exchange, defendant Drudge received a flat monthly "royalty payment" of $3,000 from AOL. During the time relevant to this case, defendant Drudge has had no other source of income. Under the licensing agreement, Drudge is to create, edit, update and "otherwise manage" the content of the Drudge Report, and AOL may "remove content that AOL reasonably determine[s] to violate AOL's then standard terms of service." Drudge transmits new editions of the Drudge Report by e-mailing them to AOL. AOL then posts the new editions on the AOL service. Drudge also has continued to distribute each new edition of the Drudge Report via e-mail and his own web site.

Late at night on the evening of Sunday, August 10, 1997 (Pacific Daylight Time), defendant Drudge wrote and transmitted the edition of the Drudge Report that contained the alleged defamatory statement about the Blumenthals. Drudge transmitted the report from Los Angeles, California by e-mail to his direct subscribers and by posting both a headline and the full text of the Blumenthal story on his world wide web site. He then 48 transmitted the text but not the headline to AOL, which in turn made it available to AOL subscribers.

After receiving a letter from plaintiffs' counsel on Monday, August 11, 1997, Complaint, Ex. 6, defendant Drudge retracted the story through a special edition of the Drudge Report posted on his web site and e-mailed to his subscribers. At approximately 2:00 a.m. on Tuesday, August 12, 1997, Drudge e-mailed the retraction to AOL which posted it on the AOL service. Defendant Drudge later publicly apologized to the Blumenthals.).

II. AOL's MOTION FOR SUMMARY JUDGMENT

... Section 230(c) of the Communications Decency Act of 1996 provides:

> 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.

47 U.S.C. § 230(c)(1). The statute goes on to define the term "information content provider" as "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(e)(3). In view of this statutory language, plaintiffs' argument that the *Washington Post* would be liable if it had done what AOL did here — "publish Drudge's story without doing anything whatsoever to edit, verify, or even read it (despite knowing what Drudge did for a living and how he did it)," — has been rendered irrelevant by Congress.

Plaintiffs concede that AOL is a "provider ... of an interactive computer service" 50 for purposes of Section 230, and that if AOL acted exclusively as a provider of an interactive computer service it may not be held liable for making the Drudge Report available to AOL subscribers. *See* 47 U.S.C. § 230(c)(1). They also concede that Drudge is an "information content provider" because he wrote the alleged defamatory material about the Blumenthals contained in the Drudge Report. While plaintiffs suggest that AOL is responsible along with Drudge because it had some role in writing or editing the material in the Drudge Report, they have provided no

factual support for that assertion. Indeed, plaintiffs affirmatively state that "no person, other than Drudge himself, edited, checked, verified, or supervised the information that Drudge published in the Drudge Report." It also is apparent to the Court that there is no evidence to support the view originally taken by plaintiffs that Drudge is or was an employee or agent of AOL, and plaintiffs seem to have all but abandoned that argument.

AOL acknowledges both that Section 230(c)(1) would not immunize AOL with respect to any information AOL developed or created entirely by itself and that there are situations in which there may be two or more information content providers responsible for material disseminated on the Internet — joint authors, a lyricist and a composer, for example. While Section 230 does not preclude joint liability for the joint development of content, AOL maintains that there simply is no evidence here that AOL had any role in creating or developing any of the information in the Drudge Report. The Court agrees. It is undisputed that the Blumenthal story was written by Drudge without any substantive or editorial involvement by AOL. AOL was nothing more than a provider of an interactive computer service on which the Drudge Report was carried, and Congress has said quite clearly that such a provider shall not be treated as a "publisher or speaker" and therefore may not be held liable in tort. 47 U.S.C. § 230(c)(1).

As Chief Judge Wilkinson recently wrote for the Fourth Circuit:

> 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. Specifically, § 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions — such as deciding whether to publish, withdraw, postpone or alter content — are barred. . . .

Zeran v. America Online, Inc., 129 F.3d 327, 330-31 (4th Cir.1997). The court in *Zeran* has provided a complete answer to plaintiffs' primary argument, an answer grounded in the statutory language and intent of Section 230.

Plaintiffs make the additional argument, however, that Section 230 of the Communications Decency Act does not provide immunity to AOL in this case because Drudge was not just an anonymous person who sent a message over the Internet through AOL. He is a person with whom AOL contracted, whom AOL paid $3,000 a month — $36,000 a year, Drudge's sole, consistent source of income — and whom AOL promoted to its subscribers and potential subscribers as a reason to subscribe to AOL. Furthermore, the license agreement between AOL and Drudge by its terms contemplates more than a passive role for AOL; in it, AOL reserves the "right to remove, or direct [Drudge] to remove, any content which, as reasonably determined by AOL ... violates AOL's then-standard Terms of Service...." By the terms of the agreement, AOL also is "entitled to require reasonable changes to ... content, to the extent such content will, in AOL's good faith judgment, adversely affect operations of the AOL network." *Id.*

In addition, shortly after it entered into the licensing agreement with Drudge, AOL issued a press release making clear the kind of material Drudge would provide to AOL subscribers — gossip and rumor — and urged potential subscribers to sign onto AOL in order to get the benefit of the Drudge Report. The press release was captioned: "AOL Hires Runaway Gossip Success Matt Drudge." It noted that "[m]averick gossip columnist Matt Drudge has teamed up with

America Online," and stated: "Giving the Drudge Report a home on America Online (keyword: Drudge) opens up the floodgates to an audience ripe for Drudge's brand of reporting.... AOL has made Matt Drudge instantly accessible to members who crave instant gossip and news breaks." Why is this different, the Blumenthals suggest, from AOL advertising and promoting a new purveyor of child pornography or other offensive material? Why should AOL be permitted to tout someone as a gossip columnist or rumor monger who will make such rumors and gossip "instantly accessible" to AOL subscribers, and then claim immunity when that person, as might be anticipated, defames another?

If it were writing on a clean slate, this Court would agree with plaintiffs. AOL has certain editorial rights with respect to the content provided by Drudge and disseminated by AOL, including the right to require changes in content and to remove it; and it has affirmatively promoted Drudge as a new source of unverified instant gossip on AOL. Yet it takes no responsibility for any damage he may cause. AOL is not a passive conduit like the telephone company, a common carrier with no control and therefore no responsibility for what is said over the telephone wires. Because it has the fight to exercise editorial control over those with whom it contracts and whose words it disseminates, it would seem only fair to hold AOL to the liability standards applied to a publisher or, at least, like a book store owner or library, to the liability standards applied to a distributor. But Congress has made a different policy choice by providing immunity even where the interactive service provider has an active, even aggressive role in making available content prepared by others. In some sort of tacit *quid pro quo* arrangement with the service provider community, Congress has conferred immunity from tort liability as an incentive to Internet service providers to self-police the Internet for obscenity and other offensive material, even where the self-policing is unsuccessful or not even attempted.

In Section 230(c)(2) of the Communications Decency Act, Congress provided:

> 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)(2). As the Fourth Circuit stated in *Zeran:* "Congress enacted § 230 to remove ... disincentives to self-regulation.... Fearing that the specter of liability would ... deter service providers from blocking and screening offensive material .... § 230 forbids the imposition of publisher liability on a service provider for the exercise of its editorial and selfregulatory functions." *Zeran v. America Online, Inc., 129 F.3d at 331* . . .

While it appears to this Court that AOL in this case has taken advantage of all the benefits conferred by Congress in the Communications Decency Act, and then some, without accepting any of the burdens that Congress intended, the statutory language is clear: AOL is immune from suit, and the Court therefore must grant its motion for summary judgment.

[The court denied Drudge's motion to dismiss for lack of personal jurisdiction.]

CLASS 11: MORE SECTION 230

Today, we continue our discussion of Section 230 with three more modern cases that illustrate contemporary disputes over how far it reaches. They deal with three quite different web sites: Roommates.com, Myspace, and AutoAdmit.com. This class continues last time's emphasis on intermediary power., with a running undercurrent of our first theme: whether online is really different than offline.

Preparation Questions:

(1) Each case for today explores a different boundary in Section 230's immunity. What are these boundaries? How are the issues these cases raise different?

(2) You may be starting to notice our fourth course theme: innovation on the Internet. I asked you last time how intermediary liability enables companies to try out certain kinds of new business models online—pay attention to this question today, as well. Where would Myspace be without Section 230? Roommates.com? AutoAdmit?

(3) Explain what the following sentence from *Doe v. Myspace* means: "Plaintiffs argue the CDA does not bar their claims against MySpace because their claims are not directed toward MySpace in its capacity as a publisher." Why does the court disagree? Does *Zeran* compel this result? What does "publisher" now mean for Section 230 purposes? What other causes of action can you think of that are now preempted?

(4) In *Roommates.com*, don't confuse the question of actual liability under the Fair Housing Act with Section 230 immunity from Fair Housing Act claims. Just because something gets past Section 230 doesn't automatically mean that it's actually a Fair Housing Act violation. It's still a fair question, though. Suppose that Section 230 didn't exist. List the things that Roommates.com and its users do; do any of them violate the Fair Housing Act, as described in the opinion?

(5) What is the distinction in *Roommates.com* between discriminatory answers to questions using drop-down menus and discriminatory answers in free-form text fields? Are you convinced? If I type "rent apartment to whites" into Google, can Google rely on Section 230? Why or why not?

(6) If you're not already familiar with Craigslist, go find out about it. Note *Craigslist's Fair Housing Act page* and its warning on every apartment search page. Under the test announced in *Roommates.com*, is Craigslist potentially liable for discriminatory housing ads its users place? Why or why not? *See Chicago Lawyers for Civil Rights v. Craigslist, Inc.*, 519 F.3d 666 (7th Cir. 2008).

(7) Let's revisit the question of bad incentives from last time. Do you think any of the various people and companies we've seen raise a Section 230 defense are acting in bad faith? Is AutoAdmit a problem with the existence of Section 230? With its scope? Does Section 230 facilitate the creation of communities dedicated to hatred? If so, is there anything we could or should do about it? Would rolling back Section 230 create chilling effects on legitimate speech online? Do our private power cases on holding intermediaries accountable have anything to teach us here?

Doe v. Myspace, Inc.
474 F. Supp. 2d 843 (W.D. Tex. 2007)

SAM SPARKS, UNITED STATES DISTRICT JUDGE.

BE IT REMEMBERED on the 1st day of February 2007, the Court held a hearing in the above-styled cause, to consider Defendants MySpace, Inc. and News Corporation's ("MySpace") Motion to Dismiss, Plaintiffs' responses thereto , and Defendants' reply thereto . Having considered the motion, the responses, the replies, the arguments of counsel at the hearing, the relevant case law, and the case file as a whole, the Court now enters the following opinion and orders.

Background

MySpace.com is the most visited web site in the United States, and it is owned by Defendant MySpace, Inc.[2] MySpace.com is a "social networking web site" that allows its members to create online "profiles," which are individual web pages on which members post photographs, videos, and information about their lives and interests. The idea of online social networking is that members will use their online profiles to become part of an online community of people with common interests. Once a member has created a profile, she can extend "friend invitations" to other members and communicate with her friends over the MySpace.com platform via e-mail, instant messaging, or blogs.

MySpace.com is free to users who agree to the MySpace Terms of Use Agreement. Every new member of MySpace.com, including Julie Doe, agrees to be bound by the MySpace.com Terms of Service, by clicking a check box on the website. MySpace's Terms of Service provide that MySpace cannot verify the age or identity of MySpace.com members and cautions members not to provide "telephone numbers, street addresses, last names, URLs or email addresses" to other members.

According to Plaintiffs' Verified Complaint, Julie Doe created a MySpace profile when she was 13 years old. At the hearing, Plaintiffs' counsel admitted that Julie Doe lied about her age and represented that she was 18 years old when she joined MySpace.com[3] Plaintiffs allege Pete. Solis, a nineteen-year-old, initiated contact with Julie Doe, then fourteen years old, through MySpace.com on April 6, 2006. Subsequently, Julie Doe provided Pete Solis with her telephone number and the two communicated over the phone for several weeks. At some point, Julie Doe and Pete Solis arranged to meet for a date on May 12, 2006. Plaintiffs allege that during that meeting Pete Solis sexually assaulted Julie Doe. On May 13, 2006, Jane Doe, Julie's mother, called the Austin Police Department to report the sexual assault of her daughter. Pete Solis was subsequently arrested and indicted by the Travis County District Attorney's Office for Sexual Assault, a second degree felony.

This case was filed in Bronx County, New York, on September 26, 2006, and subsequently removed to the United States District Court for the Southern District ofNew York on September 29, 2006. The Honorable Miriam Goldman. Cedarbaum of the United States District Court for the Southern District of New York transferred the case to this Court, pursuant to *28 U.S.C. §*

---

[2] Defendant MySpace, Inc. is wholly owned by Fox Interactive Media, Inc., a subsidiary of Defendant News Corporation.

[3] MySpace.com requires that a user be at least fourteen years old to use their services.

1404(a), on December 1, 2006. Plaintiffs' Verified Complaint, the live pleading in this case filed in Bronx County, New York, asserts the following causes of action against Defendants: negligence, gross negligence, fraud, and negligent misrepresentation.

I. Defendants' Motion to Dismiss

MySpace moves to dismiss this case with prejudice pursuant to *Federal Rule of Civil Procedure 12(b)(6)* and *9(b)*. Defendants assert they are immune from this suit under the Communications Decency Act of 1996. Defendants also assert Plaintiffs' negligence claims fail under the common law and Plaintiffs' fraud and negligent misrepresentation claims do not satisfy the heightened pleading standard of *Federal Rule of Civil Procedure 9(b)*.

A. Communications Decency Act of 1996

The Communications Decency Act of 1996, *47 U.S.C. § 230* (the "CDA" or the "Act"), 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." *47 U.S.C. § 230 (c)(1)*. Neither party contests that MySpace is an "interactive computer service" as defined by the CDA, and it is clear that MySpace meets the statutory definition of such a service. *See 47 U.S.C. § 230(f)(2)*. 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)*. It is also clear that both Julie Doe and Pete Solis qualify as "information content providers" with respect to their communications through MySpace. . . .

Despite Plaintiffs' arguments to the contrary, the Court finds *Zeran* and its rationale to be applicable to the case at hand. Here, Plaintiffs seek to impose tort liability on MySpace, a company that functions as an intermediary by providing a forum for the exchange of information between third party users. Plaintiffs' allegations that MySpace knew sexual predators were using the service to communicate with minors and failed to react appropriately can be analogized to Zeran's claims that AOL failed to act quickly enough to remove the ads and to prevent the posting of additional ads after AOL was on notice that the content was false.

Plaintiffs contend the CDA is inapplicable to their claims, so Defendants should not be granted immunity under the CDA. Plaintiffs assert *Section 230(c)(1)* is inapplicable here because Plaintiffs have not sued MySpace for the publication of third-party content but rather for failing to implement basic safety measures to prevent sexual predators from communicating with minors on MySpace. Plaintiffs attempt to distinguish *Carafano*, *Zeran*, and *Prickett v. Info USA, Inc., No. 4:05-CV-10, 2006 U.S. Dist. LEXIS 21867, 2006 WL 887431 (E.D. Tex. Mar. 30, 2006)*, from the case at hand, by pointing out that each of these cases was based on the listing of third-party content without taking into account its defamatory or inaccurate nature. Plaintiffs assert their case is not based on MySpace's posting of third-party content, but rather on MySpace's failure to institute safety measures to protect minors.

Plaintiffs seek to limit CDA immunity to cases involving defamation or related actions and assert that their claims against MySpace have nothing to do with the content of the information provided. Plaintiffs contend that neither the plain language of the CDA nor the cases interpreting it contemplate the extension of the CDA's immunity provision to MySpace in this case.

Nothing on the face of the statute supports Plaintiffs' narrow interpretation that the CDA's immunity applies only to cases involving defamation and defamation-related claims. *47 U.S.C. § 230*. The Eastern District of Texas recently addressed the application of CDA immunity in a case involving claims of negligence, negligence per se, intentional infliction of emotional distress, invasion of privacy, civil conspiracy, and distribution of child pornography. *Doe v. Bates, No. 5:05-CV-91-DF-CMC, 2006 U.S. Dist. LEXIS 93348, 2006 WL 3813758 (E.D. Tex. Dec. 27, 2006)*. This case dealt with a lawsuit against Yahoo! Inc., which arose from an e-group hosted by Yahoo! on which illegal child pornography pictures were posted by a third party. Among the photos were sexually explicit photos of Johnny Doe, a minor. The district court determined that *Section 230(c)(1)* applied to immunize Yahoo! because Plaintiffs' claims sought to treat Defendant as the "publisher or speaker" of the third-party content (the photos). *2006 U.S. Dist. LEXIS 93348, [WL] at * 2-4*. It is important to note that in *Bates*, as here, the Plaintiffs did not allege that there was anything defamatory or inaccurate about the posted content, but the court still applied the CDA to immunize Yahoo! from suit.

Defendants have presented numerous cases in which the CDA has been applied to bar non-defamation claims. *See, e.g., Ben Ezra, Weinstein & Co. v. America Online, Inc., 206 F.3d 980, 986 (10th Cir. 2000)* (negligence claim); *Zeran, 129 F.3d at 330* (negligence claims); *Bates, 2006 U.S. Dist. LEXIS 93348, 2006 WL 3813758 at *5* (negligence, negligence per se, intentional infliction of emotional distress, invasion of privacy, civil conspiracy and distribution of child pornography); *Beyond Sys., Inc. v. Keynetics, Inc., 422 F. Supp. 2d 523, 536 (D. Md. 2006)* (claim under Maryland Commercial Electronic Mail Act); *Barnes v. Yahoo!, Inc., No. Civ. 05-926-AA, 2005 U.S. Dist. LEXIS 28061, 2005 WL 3005602, at *4 (D. Or. Nov. 8, 2005)* (negligence claim resulting in personal injury). All of these cases involved attempts to hold an interactive computer service liable for its publication of third-party content or harms flowing from the dissemination of that content.

Plaintiffs argue the CDA does not bar their claims against MySpace because their claims are not directed toward MySpace in its capacity as a publisher. Plaintiffs argue this suit is based on MySpace's negligent failure to take reasonable safety measures to keep young children off of its site and not based, on MySpace's editorial acts. The Court, however, finds this artful pleading to be disingenuous. It is quite obvious the underlying basis of Plaintiffs' claims is that, through postings on MySpace, Pete Solis and Julie Doe met and exchanged personal information which eventually led to an in-person meeting and the sexual assault of Julie Doe. If MySpace had not published communications between Julie Doe and Solis, including personal contact information, Plaintiffs assert they never would have met and the sexual assault never would have occurred. No matter how artfully Plaintiffs seek to plead their claims, the Court views Plaintiffs' claims as directed toward MySpace in its publishing, editorial, and/or screening capacities. Therefore, in accordance with the cases cited above, Defendants are entitled to immunity under the CDA, and the Court dismisses Plaintiffs' negligence and gross negligence claims with prejudice under *rule 12(c) of the Federal Rules of Civil Procedure*.

i. Self-Regulation

In addition to the protection afforded to interactive computer services in their publishing capacity, the CDA also immunizes such services from liability based on efforts to self-regulate material. Specifically, "[n]o provider or user of an interactive computer service shall be held liable on account of—(A) any action voluntarily taken in good fath 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 . . . ." *47 U.S.C. § 230(c)(2)(A)*. This section reflects Congress's recognition that the potential for liability attendant to implementing safety features and policies created a disincentive for interactive computer services to implement any safety features or policies at all. To the extent Plaintiffs seek to hold MySpace liable for ineffective security measures and/or policies relating to age verification,[6] the Court alternately finds such claims are barred under *§ 230(c)(2)(A)*. . . .

Fair Housing Council v. Roommates.com, LLC
521 F.3d 1157 (9th Cir. 2008) (en banc)

KOZINSKI, Chief Judge:

We plumb the depths of the immunity provided by section 230 of the Communications Decency Act of 1996 ("CDA").

Facts[1]

Defendant Roommate.com, LLC ("Roommate") operates a website designed to match people renting out spare rooms with people looking for a place to live.[2] At the time of the district court's disposition, Roommate's website featured approximately 150,000 active listings and received around a million page views a day. Roommate seeks to profit by collecting revenue from advertisers and subscribers.

Before subscribers can search listings or post[3] housing opportunities on Roommate's website, they must create profiles, a process that requires them to answer a series of questions. In addition to requesting basic information—such as name, location and email address—Roommate requires each subscriber to disclose his sex, sexual orientation and whether he would bring children to a household. Each subscriber must also describe his preferences in roommates with respect to the same three criteria: sex, sexual orientation and whether they will bring children to the household. The site also encourages subscribers to provide "Additional Comments" describing themselves and their desired roommate in an open-ended essay. After a new subscriber completes the application, Roommate assembles his answers into a "profile page." The profile page displays the subscriber's pseudonym, his description and his preferences, as divulged through answers to Roommate's questions.

Subscribers can choose between two levels of service: Those using the site's free service level can create their own personal profile page, search the profiles of others and send personal email messages. They can also receive periodic emails from Roommate, informing them of available housing opportunities matching their preferences. Subscribers who pay a monthly fee also gain

---

[6] The Court finds Plaintiffs' claims particularly unwarranted here given that Julie Doe lied about her actual age to bypass the age requirement and then violated MySpace's express rules by giving out her personal information.

[1] This appeal is taken from the district court's order granting defendant's motion for summary judgment, so we view contested facts in the light most favorable to plaintiffs. See Winterrowd v. Nelson, 480 F.3d 1181, 1183 n.3 (9th Cir. 2007)

[2] For unknown reasons, the company goes by the singular name "Roommate.com, LLC" but pluralizes its website's URL, www.roommates.com.

[3] In the online context, "posting" refers to providing material that can be viewed by other users, much as one "posts" notices on a physical bulletin board.

the ability to read emails from other users, and to view other subscribers' "Additional Comments."

The Fair Housing Councils of the San Fernando Valley and San Diego ("Councils") sued Roommate in federal court, alleging that Roommate's business violates the federal Fair Housing Act ("FHA"), 42 U.S.C. § 3601 et seq., and California housing discrimination laws.[4] Councils claim that Roommate is effectively a housing broker doing online what it may not lawfully do off-line. The district court held that Roommate is immune under section 230 of the CDA, 47 U.S.C. § 230(c), and dismissed the federal claims without considering whether Roommate's actions violated the FHA. The court then declined to exercise supplemental jurisdiction over the state law claims. Councils appeal the dismissal of the FHA claim and Roommate cross-appeals the denial of attorneys' fees.

Analysis

Section 230 of the CDA immunizes providers of interactive computer services[6] against liability arising from content created by third parties: "No provider . . . of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c).[7] This grant of immunity applies only if the interactive computer service provider is not also an "information content provider," which is defined as someone who is "responsible, in whole or in part, for the creation or development of" the offending content. Id. § 230(f)(3).

A website operator can be both a service provider and a content provider: If it passively displays content that is created entirely by third parties, then it is only a service provider with respect to that content. But as to content that it creates itself, or is "responsible, in whole or in part" for creating or developing, the website is also a content provider. Thus, a website may be immune from liability for some of the content it displays to the public but be subject to liability for other content. . . .

[The court reviews pre-CDA caselaw.]

In passing section 230, Congress sought to spare interactive computer services this grim choice by allowing them to perform some editing on user-generated content without thereby becoming liable for all defamatory or otherwise unlawful messages that they didn't edit or delete. In other words, Congress sought to immunize the removal of user-generated content, not the creation of content: "[S]ection [230] provides 'Good Samaritan' protections from civil liability for providers . . . of an interactive computer service for actions to restrict . . . access to objectionable online material. One of the specific purposes of this section is to overrule Stratton-

---

[4] The Fair Housing Act prohibits certain forms of discrimination on the basis of "race, color, religion, sex, familial status, or national origin." 42 U.S.C. § 3604(c). The California fair housing law prohibits discrimination on the basis of "sexual orientation, marital status, . . . ancestry, . . . source of income, or disability," in addition to reiterating the federally protected classifications. Cal. Gov. Code § 12955.

[6] Section 230 defines an "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server." 47 U.S.C. § 230(f)(2); see Carafano v. Metrosplash.com, Inc., 207 F. Supp. 2d 1055, 1065-66 (C.D. Cal. 2002) (an online dating website is an "interactive computer service" under the CDA), aff'd, 339 F.3d 1119 (9th Cir. 2003). Today, the most common interactive computer services are websites. Councils do not dispute that Roommate's website is an interactive computer service.

[7] The Act also gives immunity to users of third-party content. This case does not involve any claims against users so we omit all references to user immunity when quoting and analyzing the statutory text.

Oakmont [sic] v. Prodigy and any other similar decisions which have treated such providers . . . as publishers or speakers of content that is not their own because they have restricted access to objectionable material." H.R. Rep. No. 104-458 (1996) (Conf. Rep.), as reprinted in 1996 U.S.C.C.A.N. 10 (emphasis added). Indeed, the section is titled "Protection for 'good samaritan' blocking and screening of offensive material" and, as the Seventh Circuit recently held, the substance of section 230(c) can and should be interpreted consistent with its caption. Chi. Lawyers' Comm. for Civ. Rights Under Law, Inc. v. Craigslist, Inc., No. 07- 1101, 519 F.3d 666, 2008 U.S. App. LEXIS 5472, slip op. at 6 (7th Cir. Mar. 14, 2008) (quoting Doe v. GTE Corp., 347 F.3d 655, 659-60 (7th Cir. 2003)).

With this backdrop in mind, we examine three specific functions performed by Roommate that are alleged to violate the Fair Housing Act and California law.

1. Councils first argue that the questions Roommate poses to prospective subscribers during the registration process violate the Fair Housing Act and the analogous California law. Councils allege that requiring subscribers to disclose their sex, family status and sexual orientation "indicates" an intent to discriminate against them, and thus runs afoul of both the FHA and state law.[13]

Roommate created the questions and choice of answers, and designed its website registration process around them. Therefore, Roommate is undoubtedly the "information content provider" as to the questions and can claim no immunity for posting them on its website, or for forcing subscribers to answer them as a condition of using its services.

Here we must determine whether Roommate has immunity under the CDA because Councils have at least a plausible claim that Roommate violated state and federal law by merely posing the questions. We need not decide whether any of Roommate's questions actually violate the Fair Housing Act or California law, or whether they are protected by the First Amendment or other constitutional guarantees, see craigslist, 2008 U.S. App. LEXIS 5472, *11; we leave those issues for the district court on remand. Rather, we examine the scope of plaintiffs' substantive claims only insofar as necessary to determine whether section 230 immunity applies. However, we note that asking questions certainly can violate the Fair Housing Act and analogous laws in the physical world. For example, a real estate broker may not inquire as to the race of a prospective buyer, and an employer may not inquire as to the religion of a prospective employee. If such questions are unlawful when posed face-to-face or by telephone, they don't magically become lawful when asked electronically online. The Communications Decency Act was not meant to create a lawless no-man's-land on the Internet.

Councils also claim that requiring subscribers to answer the questions as a condition of using Roommate's services unlawfully "cause[s]" subscribers to make a "statement . . . with respect to the sale or rental of a dwelling that indicates [a] preference, limitation, or discrimination," in violation of 42 U.S.C. § 3604(c). The CDA does not grant immunity for inducing third parties to express illegal preferences. Roommate's own acts—posting the

---

[13] The Fair Housing Act prohibits any "statement . . . with respect to the sale or rental of a dwelling that indicates . . . an intention to make [a] preference, limitation, or discrimination" on the basis of a protected category. 42 U.S.C. § 3604(c) (emphasis added). California law prohibits "any written or oral inquiry concerning the" protected status of a housing seeker. Cal. Gov. Code § 12955(b).

questionnaire and requiring answers to it—are entirely its doing and thus section 230 of the CDA does not apply to them. Roommate is entitled to no immunity.

2. Councils also charge that Roommate's development and display of subscribers' discriminatory preferences is unlawful. Roommate publishes a "profile page" for each subscriber on its website. The page describes the client's personal information—such as his sex, sexual orientation and whether he has children—as well as the attributes of the housing situation he seeks. The content of these pages is drawn directly from the registration process: For example, Roommate requires subscribers to specify, using a drop-down menu[17] provided by Roommate, whether they are "Male" or "Female" and then displays that information on the profile page. Roommate also requires subscribers who are listing available housing to disclose whether there are currently "Straight male(s)," "Gay male(s)," "Straight female(s)" or "Lesbian(s)" living in the dwelling. Subscribers who are seeking housing must make a selection from a drop-down menu, again provided by Roommate, to indicate whether they are willing to live with "Straight or gay" males, only with "Straight" males, only with "Gay" males or with "No males." Similarly, Roommate requires subscribers listing housing to disclose whether there are "Children present" or "Children not present" and requires housing seekers to say "I will live with children" or "I will not live with children." Roommate then displays these answers, along with other information, on the subscriber's profile page. This information is obviously included to help subscribers decide which housing opportunities to pursue and which to bypass. In addition, Roommate itself uses this information to channel subscribers away from listings where the individual offering housing has expressed preferences that aren't compatible [**16] with the subscriber's answers.

The dissent tilts at windmills when it shows, quite convincingly, that Roommate's subscribers are information content providers who create the profiles by picking among options and providing their own answers. Dissent at 3485-88. There is no disagreement on this point. But, the fact that users are information content providers does not preclude Roommate from also being an information content provider by helping "develop" at least "in part" the information in the profiles. As we explained in Batzel, the party responsible for putting information online may be subject to liability, even if the information originated with a user. See Batzel v. Smith, 333 F.3d 1018, 1033 (9th Cir. 2003).

Here, the part of the profile that is alleged to offend the Fair Housing Act and state housing discrimination laws—the information about sex, family status and sexual orientation—is provided by subscribers in response to Roommate's questions, which they cannot refuse to answer if they want to use defendant's services. By requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers, Roommate becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information. And section 230 provides immunity only if the interactive computer service does not "creat[e] or develop[ ]" the information "in whole or in part." See 47 U.S.C. § 230(f)(3).

Our dissenting colleague takes a much narrower view of what it means to "develop" information online, and concludes that Roommate does not develop the information because "[a] ll Roommate does is to provide a form with options for standardized answers." Dissent at 3487. But Roommate does much more than provide options. To begin with, it asks discriminatory

---

[17] A drop-down menu allows a subscriber to select answers only from among options provided by the website.

questions that even the dissent grudgingly admits are not entitled to CDA immunity. Dissent at 3480 n.5. The FHA makes it unlawful to ask certain discriminatory questions for a very good reason: Unlawful questions solicit (a.k.a. "develop") unlawful answers. Not only does Roommate ask these questions, Roommate makes answering the discriminatory questions a condition of doing business. This is no different from a real estate broker in real life saying, "Tell me whether you're Jewish or you can find yourself another broker." When a business enterprise extracts such information from potential customers as a condition of accepting them as clients, it is no stretch to say that the enterprise is responsible, at least in part, for developing that information. For the dissent to claim that the information in such circumstances is "created solely by" the customer, and that the business has not helped in the least to develop it, Dissent at 3487-88, strains both credulity and English.

Roommate also argues that it is not responsible for the information on the profile page because it is each subscriber's action that leads to publication of his particular profile—in other words, the user pushes the last button or takes the last act before publication. We are not convinced that this is even true, but don't see why it matters anyway. The projectionist in the theater may push the last button before a film is displayed on the screen, but surely this doesn't make him the sole producer of the movie. By any reasonable use of the English language, Roommate is "responsible" at least "in part" for each subscriber's profile page, because every such page is a collaborative effort between Roommate and the subscriber.

Similarly, Roommate is not entitled to CDA immunity for the operation of its search system, which filters listings, or of its email notification system, which directs emails to subscribers according to discriminatory criteria.[21] Roommate designed its search system so it would steer users based on the preferences and personal characteristics that Roommate itself forces subscribers to disclose. If Roommate has no immunity for asking the discriminatory questions, as we concluded above, see pp. 3455-57 supra, it can certainly have no immunity for using the answers to the unlawful questions to limit who has access to housing.

For example, a subscriber who self-identifies as a "Gay male" will not receive email notifications of new housing opportunities supplied by owners who limit the universe of acceptable tenants to "Straight male(s)," "Straight female(s)" and "Lesbian(s)." Similarly, subscribers with children will not be notified of new listings where the owner specifies "no children." Councils charge that limiting the information a subscriber can access based on that subscriber's protected status violates the Fair Housing Act and state housing discrimination laws. It is, Councils allege, no different from a real estate broker saying to a client: "Sorry, sir, but I can't show you any listings on this block because you are [gay/female/black/a parent]." If such screening is prohibited when practiced in person or by telephone, we see no reason why Congress would have wanted to make it lawful to profit from it online.

Roommate's search function is similarly designed to steer users based on discriminatory criteria. Roommate's search engine thus differs materially from generic search engines such as Google, Yahoo! and MSN Live Search, in that Roommate designed its system to use allegedly unlawful criteria so as to limit the results of each search, and to force users to participate in its discriminatory process. In other words, Councils allege that Roommate's search is designed to

---

[21] Other circuits have held that it is unlawful for housing intermediaries to "screen" prospective housing applicants on the basis of race, even if the preferences arise with landlords. See Jeanty v. McKey & Poague, Inc., 496 F.2d 1119, 1120-21 (7th Cir. 1974).

make it more difficult or impossible for individuals with certain protected characteristics to find housing—something the law prohibits. By contrast, ordinary search engines do not use unlawful criteria to limit the scope of searches conducted on them, nor are they designed to achieve illegal ends—as Roommate's search function is alleged to do here. Therefore, such search engines play no part in the "development" of any unlawful searches. See 47 U.S.C. § 230(f)(3).

It's true that the broadest sense of the term "develop" could include the functions of an ordinary search engine—indeed, just about any function performed by a website. But to read the term so broadly would defeat the purposes of section 230 by swallowing up every bit of the immunity that the section otherwise provides. At the same time, reading the exception for co-developers as applying only to content that originates entirely with the website—as the dissent would seem to suggest—ignores the words "development . . . in part" in the statutory passage "creation or development in whole or in part." 47 U.S.C. § 230(f)(3) (emphasis added). We believe that both the immunity for passive conduits and the exception for co-developers must be given their proper scope and, to that end, we interpret the term "development" as referring not merely to augmenting the content generally, but to materially contributing to its alleged unlawfulness. In other words, a website helps to develop unlawful content, and thus falls within the exception to section 230, if it contributes materially to the alleged illegality of the conduct. . . .

In an abundance of caution, and to avoid the kind of misunderstanding the dissent seems to encourage, we offer a few examples to elucidate what does and does not amount to "development" under section 230 of the Communications Decency Act: If an individual uses an ordinary search engine to query for a "white roommate," the search engine has not contributed to any alleged unlawfulness in the individual's conduct; providing neutral tools to carry out what may be unlawful or illicit searches does not amount to "development" for purposes of the immunity exception. A dating website that requires users to enter their sex, race, religion and marital status through drop-down menus, and that provides means for users to search along the same lines, retains its CDA immunity insofar as it does not contribute to any alleged illegality; this immunity is retained even if the website is sued for libel based on these characteristics because the website would not have contributed materially to any alleged defamation. Similarly, a housing website that allows users to specify whether they will or will not receive emails by means of user-defined criteria might help some users exclude email from other users of a particular race or sex. However, that website would be immune, so long as it does not require the use of discriminatory criteria. A website operator who edits user-created content—such as by correcting spelling, removing obscenity or trimming for length—retains his immunity for any illegality in the user-created content, provided that the edits are unrelated to the illegality. However, a website operator who edits in a manner that contributes to the alleged illegality—such as by removing the word "not" from a user's message reading "[Name] did not steal the artwork" in order to transform an innocent message into a libelous one—is directly involved in the alleged illegality and thus not immune.

Here, Roommate's connection to the discriminatory filtering process is direct and palpable: Roommate designed its search and email systems to limit the listings available to subscribers based on sex, sexual orientation and presence of children. Roommate selected the criteria used to hide listings, and Councils allege that the act of hiding certain listings is itself unlawful under the Fair Housing Act, which prohibits brokers from steering clients in accordance with discriminatory preferences. We need not decide the merits of Councils' claim to hold that Roommate is

sufficiently involved with the design and operation of the search and email systems—which are engineered to limit access to housing on the basis of the protected characteristics elicited by the registration process—so as to forfeit any immunity to which it was otherwise entitled under section 230. . . .

3. Councils finally argue that Roommate should be held liable for the discriminatory statements displayed in the "Additional Comments" section of profile pages. At the end of the registration process, on a separate page from the other registration steps, Roommate prompts subscribers to "tak[e] a moment to personalize your profile by writing a paragraph or two describing yourself and what you are looking for in a roommate." The subscriber is presented with a blank text box, in which he can type as much or as little about himself as he wishes. Such essays are visible only to paying subscribers.

Subscribers provide a variety of provocative, and often very revealing, answers. The contents range from subscribers who "[p]ref[er] white Male roommates" or require that "[t]he person applying for the room MUST be a BLACK GAY MALE" to those who are "NOT looking for black muslims." Some common themes are a desire to live without "drugs, kids or animals" or "smokers, kids or druggies," while a few subscribers express more particular preferences, such as preferring to live in a home free of "psychos or anyone on mental medication." Some subscribers are just looking for someone who will get along with their significant other[34] or with their most significant Other.[35]

Roommate publishes these comments as written.[36] It does not provide any specific guidance as to what the essay should contain, nor does it urge subscribers to input discriminatory preferences. Roommate is not responsible, in whole or in part, for the development of this content, which comes entirely from subscribers and is passively displayed by Roommate. Without reviewing every essay, Roommate would have no way to distinguish unlawful discriminatory preferences from perfectly legitimate statements. Nor can there be any doubt that this information was tendered to Roommate for publication online. See pp. 3466-67 supra. This is precisely the kind of situation for which section 230 was designed to provide immunity. See pp. 3453-3455 supra.

The fact that Roommate encourages subscribers to provide something in response to the prompt is not enough to make it a "develop[er]" of the information under the common-sense interpretation of the term we adopt today. It is entirely consistent with Roommate's business model to have subscribers disclose as much about themselves and their preferences as they are willing to provide. But Roommate does not tell subscribers what kind of information they should or must include as "Additional Comments," and certainly does not encourage or enhance any

---

[34] "The female we are looking for hopefully wont [sic] mind having a little sexual incounter [sic] with my boyfriend and I [very sic]."

[35] "We are 3 Christian females who Love our Lord Jesus Christ . . . . We have weekly bible studies and bi-weekly times of fellowship."

[36] It is unclear whether Roommate performs any filtering for obscenity or "spam," but even if it were to perform this kind of minor editing and selection, the outcome would not change. See Batzel, 333 F.3d at 1031.

discriminatory content created by users. Its simple, generic prompt does not make it a developer of the information posted.[37]

Councils argue that—given the context of the discriminatory questions presented earlier in the registration process—the "Additional Comments" prompt impliedly suggests that subscribers should make statements expressing a desire to discriminate on the basis of protected classifications; in other words, Councils allege that, by encouraging some discriminatory preferences, Roommate encourages other discriminatory preferences when it gives subscribers a chance to describe themselves. But the encouragement that bleeds over from one part of the registration process to another is extremely weak, if it exists at all. Such weak encouragement cannot strip a website of its section 230 immunity, lest that immunity be rendered meaningless as a practical matter.[38]

We must keep firmly in mind that this is an immunity statute we are expounding, a provision enacted to protect websites against the evil of liability for failure to remove offensive content. See pp. 3453-3455 supra. Websites are complicated enterprises, and there will always be close cases where a clever lawyer could argue that something the website operator did encouraged the illegality. Such close cases, we believe, must be resolved in favor of immunity, lest we cut the heart out of section 230 by forcing websites to face death by ten thousand duck-bites, fighting off claims that they promoted or encouraged—or at least tacitly assented to—the illegality of third parties. Where it is very clear that the website directly participates in developing the alleged illegality—as it is clear here with respect to Roommate's questions, answers and the resulting profile pages—immunity will be lost. But in cases of enhancement by implication or development by inference—such as with respect to the "Additional Comments" here—section 230 must be interpreted to protect websites not merely from ultimate liability, but from having to fight costly and protracted legal battles.

The dissent prophesies doom and gloom for countless Internet services, Dissent at 3490-91, but fails to recognize that we hold part of Roommate's service entirely immune from liability. The search engines the dissent worries about, id., closely resemble the "Additional Comments" section of Roommate's website. Both involve a generic text prompt with no direct encouragement to perform illegal searches or to publish illegal content. We hold Roommate immune and there is no reason to believe that future courts will have any difficulty applying this principle. The message to website operators is clear: If you don't encourage illegal content, or design your website to require users to input illegal content, you will be immune.

We believe that this distinction is consistent with the intent of Congress to preserve the free-flowing nature of Internet speech and commerce without unduly prejudicing the enforcement of other important state and federal laws. When Congress passed section 230 it didn't intend to prevent the enforcement of all laws online; rather, it sought to encourage interactive computer services that provide users neutral tools to post content online to police that content without fear

---

[37] Nor would Roommate be the developer of discriminatory content if it provided a free-text search that enabled users to find keywords in the "Additional Comments" of others, even if users utilized it to search for discriminatory keywords. Providing neutral tools for navigating websites is fully protected by CDA immunity, absent substantial affirmative conduct on the part of the website creator promoting the use of such tools for unlawful purposes.

[38] It's true that, under a pedantic interpretation of the term "develop," any action by the website—including the mere act of making a text box available to write in—could be seen as "develop[ing]" content. However, we have already rejected such a broad reading of the term "develop" because it would defeat the purpose of section 230. See pp. 3461-64 supra.

that through their "good samaritan . . . screening of offensive material," 47 U.S.C. § 230(c), they would become liable for every single message posted by third parties on their website. ...

In light of our determination that the CDA does not provide immunity to Roommate for all of the content of its website and email newsletters, we remand for the district court to determine in the first instance whether the alleged actions for which Roommate is not immune violate the Fair Housing Act, 42 U.S.C. § 3604(c). We vacate the dismissal of the state law claims so that the district court may reconsider whether to exercise its supplemental jurisdiction in light of our ruling on the federal claims. Fredenburg v. Contra Costa County Dep't of Health Servs., 172 F. 3d 1176, 1183 (9th Cir. 1999). We deny Roommate's cross-appeal of the denial of attorneys' fees and costs; Councils prevail on some of their arguments before us so their case is perforce not frivolous.

[Partial concurrence and partial dissent of Judge McKeown omitted.]

AutoAdmit Section 230 Problem

Please read the complaint in *Doe I v. Ciolli*, No. 3:07-cv-00909 (D. Conn. complaint filed June 8, 2007), *available at* http://docs.justia.com/cases/federal/district-courts/connecticut/ctdce/3:2007cv00909/78132/1/0.pdf. Note that the complaint names Anthony Ciolli a s defendant, along with a collection of pseudonymous posters, but not Jarret Cohen.

(1) What do you think of Doe I and Doe II's case against the individual posters? Which ones?

(2) Based on what you have seen of Section 230, is Anthony Ciolli a proper defendant? If he moves the court to dismiss the complaint under FRCP 12(b)(6) for failure to state a claim upon which relief can be granted, how should the court rule?

(3) Why is Jarret Cohen not named as a defendant? What was (or should have been) the plaintiffs' litigation strategy?