Internet Law: Cases & Problems (Jan. 2015 draft)

Chapter 3: Speech

This chapter considers how the Internet affects the balances struck by free speech law. By changing the facts of how people communicate, software can unsettle existing legal doctrines. In particular, some have argued that new computer technologies undermine law by making it harder to enforce laws restricting speech, while others celebrate the open and uninhibited quality of online debates.

A. What Is "Speech"?

At first glance, one might think that there is nothing new here: speech is speech, regardless of the medium that conveys it. But the novelty of online media can call this assumption into question. Courts have struggled to understand how online speech works; indeed, in some cases, it is far from clear what even counts as "speech." *Bland* and *Bernstein* concern the reach of the First Amendment's protection for speech on the Internet; they both turn on the threshold question of whether the challenged behavior contains protected "speech." *Too Much Media* is a little different. There, the speech itself is not directly at issue. Instead, an online speaker is claiming that she is entitled to a state statutory right enjoyed by newspaper and television journalists: the privilege not to name her sources in court. All three cases raise difficult questions about the differences between offline and online activities.

United States Constitution, Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

Question

What is "speech"?

Texas v. Johnson

491 U.S. 397 (1989)

Justice Brennan delivered the opinion of the Court:

After publicly burning an American flag as a means of political protest, Gregory Lee Johnson was convicted of desecrating a flag in violation of Texas law. This case presents the question whether his conviction is consistent with the First Amendment. We hold that it is not. ...

In deciding whether particular conduct possesses sufficient communicative elements to bring the First Amendment into play, we have asked whether "[a]n intent to convey a particularized message was present, and [whether] the likelihood was great that the message would be understood by those who viewed it." *Spence v. Washington*, 418 U. S. 405, 410-411 (1974).

Bland v. Roberts

857 F. Supp. 2d 599 (E.D. Va. 2012)

Jackson, District Judge: ...

I. Factual & Procedural History

Plaintiffs ... were employed in the Hampton Sheriff's Office ("the Office"). ... The Sheriff of the Office, B.J. Roberts ("the Sheriff"), was slated for re-election in November 2009. The Plaintiffs claim that during his tenure the Sheriff used his authority to bolster his reelection efforts, including using employees to manage his political activities, using prisoners to set up campaign events and forcing his employees to sell and buy tickets to campaign fundraisers. Plaintiffs contend that in late 2009, the Sheriff learned that a number of his employees were actively supporting Jim Adams, one of the Sheriff's opponents in the election. ...

The Plaintiffs further allege that the Sheriff learned that each of them affirmatively expressed their support for Adams by informing other individuals of their support, attending a cookout which Adams also attended and "liking" Adams' Facebook page. According to the Plaintiffs, after learning of their support of his opponent, the Sheriff called a meeting in which he informed his employees that they should get on the "long train" with him rather than riding the "short train" with his opponent.

The Sheriff won the November 2009 election, and he decided not to retain the six Plaintiffs as well as six other employees. The Sheriff claims he did not reappoint three civilian employees (including Plaintiffs Bland and Woodward) based on a reduction in the number of sworn deputies which the Compensation Board allocated to him. He contends that he wanted to replace the civilian employees with sworn deputies. The Sheriff also declined to retain the remaining four deputy Plaintiffs and five other deputies for unsatisfactory work performance or for his belief that their actions "hindered the harmony and efficiency of the Office." ...

III. Discussion

A. Freedom of Speech Retaliation Claim

Plaintiffs first allege that the Sheriff failed to reappoint them in retaliation for their exercise of their right to freedom of speech when they choose to support the Sheriff's opponent in the election. In order to prove that an adverse employment action violated their First Amendment right to freedom of speech, the Plaintiffs must satisfy the three-prong test the United States Court of Appeals for the Fourth Circuit ("the Fourth Circuit") laid out in *McVey v. Stacy*, 157 F.3d 271 (4th Cir. 1998):

> Thus, to determine whether a public employee has stated a claim under the First Amendment for retaliatory discharge, we must determine (1) whether the public employee was speaking as a citizen upon a matter of public concern or as an employee about a personal matter of personal interest; (2) whether the employee's interest in speaking upon the matter of public concern outweighed the government's interest in providing effective and efficient services to the public; and (3) whether the employee's speech was a substantial factor in the employee's termination decision.

Id. at 277–78.

The first prong of the *McVey* test necessarily requires that speech exists before an evaluation of the remaining prongs can occur. Plaintiffs Carter, McCoy, and Woodward have not sufficiently alleged that they engaged in expressive speech ... . Therefore, these Plaintiffs' claims fail as a matter of law.

a. *Daniel Ray Carter, Jr. & Robert McCoy*

Carter and McCoy each allege that they engaged in constitutionally protected speech when they "made statements" on Adams' Facebook page. McCoy's Facebook activity is more nebulous than Carter's. McCoy claims that he posted a message on Adams' Facebook page which he later took down. The Court, however, is unaware of the content of this message. McCoy's barebones assertion that he made some statement at some time is insufficient evidence for the Court to adequately evaluate his claim. Without more, the Court will not speculate as to what McCoy's actual statement might have been. McCoy has not sufficiently alleged any constitutionally protected speech.

Carter alleged that he sent a statement of support and attached the statement as an exhibit to his declaration in this case. However, after reviewing the record, the Court has not found any evidence of the "statement of support" Carter allegedly made. In fact, the only evidence regarding Carter's activity on Adams' Facebook page is that he "liked" Adams' page.

It is clear, based on the Sheriffs own admissions, that at some point he became aware of McCoy and Carter's presence on Adams' Facebook page. However, the Sheriff's knowledge of the posts only becomes relevant if the Court finds the activity of liking a Facebook page to be constitutionally protected. It is the Court's conclusion that merely "liking" a Facebook page is insufficient speech to merit constitutional protection. In cases where courts have found that constitutional speech protections extended to Facebook posts, actual statements existed within the record. For example, in *Mattingly v. Milligan,* Mattingly posted on her Facebook wall referring directly to the firing of various employees. No. 4:11CV00215, 2011 WL 5184283, at *2–*3 (E.D. Ark. Nov. 1, 2011) ("Two minutes after this post, Mattingly posted another comment: 'I am trying [sic] my heart goes out to the ladies in my office that were told by letter they were no longer needed ... It's sad.'"). There, the court held that Mattingly's specific post was an expression of constitutionally protected speech. *Id.* at *3–*4. Similarly, in *Gresham v. City of Atlanta,* the plaintiff posted: "Who would like to hear the story of how I arrested a forgery perp at Best Buy online to find out later at the precinct that he was the nephew of an Atlanta Police Investigator ... ?" No. 1:10–CV–1301–RWS–ECS, 2011 WL 4601022, at *2 (N.D. Ga. Aug. 29, 2011), *report and recommendation adopted in part, rejected in part on other grounds by,* No. 1:10–CV–1301 RWS, 2011 WL 4601020 (N.D. Ga. Sep. 30, 2011). In *Gresham,* the district court adopted the Magistrate Judge's recommendation that although the statement was a close question, it constituted enough speech to be considered speaking out as a matter of public concern.

These illustrative cases differ markedly from the case at hand in one crucial way: Both *Gresham* and *Mattingly* involved actual statements. No such statements exist in this case. Simply liking a Facebook page is insufficient. It is not the kind of substantive statement that has previously warranted constitutional protection. The Court will not attempt to infer the actual content of Carter's posts from one click of a button on Adams' Facebook page. For the Court to assume that the Plaintiffs made some specific statement without evidence of such statements is improper. Facebook posts *can* be considered matters of public concern; however, the Court does not believe Plaintiffs Carter and McCoy have alleged sufficient speech to garner First Amendment protection.

Bland v. Roberts

730 F. 3d 368 (4th Cir. 2013)

Traxler, Chief Judge: ...

Here, Carter visited the Jim Adams's campaign Facebook page (the "Campaign Page"), which was named "Jim Adams for Hampton Sheriff," and he clicked the "like" button on the Campaign Page. When he did so, the Campaign Page's name and a photo of Adams — which an Adams campaign representative had selected as the Page's icon — were added to Carter's profile, which all Facebook users could view. On Carter's profile, the Campaign Page name served as a link to the Campaign Page. Carter's clicking on the "like" button also caused an announcement that Carter liked the Campaign Page to appear in the news feeds of Carter's friends. And it caused Carter's name and his profile photo to be added to the Campaign Page's "People [Who] Like This" list.

Once one understands the nature of what Carter did by liking the Campaign Page, it becomes apparent that his conduct qualifies as speech. On the most basic level, clicking on the "like" button literally causes to be published the statement that the User "likes" something, which is itself a substantive statement. In the context of a political campaign's Facebook page, the meaning that the user approves of the candidacy whose page is being liked is unmistakable. That a user may use a single mouse click to produce that message that he likes the page instead of typing the same message with several individual key strokes is of no constitutional significance.

Aside from the fact that liking the Campaign Page constituted pure speech, it also was symbolic expression. The distribution of the universally understood "thumbs up" symbol in association with Adams's campaign page, like the actual text that liking the page produced, conveyed that Carter supported Adams's candidacy. *See Spence v. Washington,* 418 U.S. 405, 410-11 (1974) (per curiam) (holding that person engaged in expressive conduct when there was "[a]n intent to convey a particularized message ... , and in the surrounding circumstances the likelihood was great that the message would be understood by those who viewed it").

In sum, liking a political candidate's campaign page communicates the user's approval of the candidate and supports the campaign by associating the user with it. In this way, it is the Internet equivalent of displaying a political sign in one's front yard, which the Supreme Court has held is substantive speech. *See City of Ladue v. Gilleo*, 512 U.S. 43, 54-56 (1994). Just as Carter's placing an "Adams for Sheriff" sign in his front yard would have conveyed to those passing his home that he supported Adams's campaign, Carter's liking Adams's Campaign Page conveyed that message to those viewing his profile or the Campaign Page. In fact, it is hardly surprising that the record reflects that this is exactly how Carter's action was understood. *See* J.A. 160 (McCoy's testimony that in light of Carter's liking Adams's Campaign Page, "everybody was saying that ... Carter is out of there because he supported Adams openly"); *see also* J.A. 793 (Sheriff's Office employee stating that Roberts had said that "certain employees were on the Facebook page of his opponent, Jim Adams, indicating their support of Adams for Sheriff").

Questions

1. What does a "like" mean?

2. McCoy and Carter's continued employment hinges on whether Facebook likes are speech. How else might the question of First Amendment coverage for Facebook likes come up?

3. The National Labor Relations Act protects employees' right "to engage in ... concerted activities for the purpose of collective bargaining or other mutual aid or protection." 29 U.S.C. § 157. A bartender at a sports bar posts to her Facebook page, "Maybe someone should do the owners of Triple Play a favor and buy it from them. They can't even do the tax paperwork correctly!!! Now I OWE money . . . Wtf!!!!" A cook responds by clicking "Like" on the post. Are these protected "concerted activities" or can the two be fired? Does it matter whether employees have been complaining to each other at work about the Triple Play's tax withholding?

4. Schools may not discipline students for speech at school unless the speech "will materially and substantially disrupt the work and discipline of the school." *Tinker v. Des Moines Independent Community School Dist.*, 393 U.S. 503, 509 (1969). How should this test apply to speech on social media? Is Facebook "on campus" or off campus," or is that distinction itself beside the point? Here are some examples; should they lead to discipline?

- L.W., a high-school student, send sends MySpace instant messages to a friend, who is concerned enough to forward them to a school administrator:

> "its pretty simple / i have a sweet gun / my neighbor is giving me 500 rounds / dhs[*] is gay / ive watched these kinds of movies so i know how NOT to go wrong / i just cant decide who will be on my hit list / and thats totally deminted and it scares even my self"

- J.S. and K.L., both eighth gradfers, create a fake MySpace using their principal's official photograph from the school's website (although not his name or the school's name), and listing his interests as:

> "detention, being a tight ass, riding the fraintrain, spending time with my child (who looks like a gorilla), baseball, my golden pen, fucking in my office, hitting on students and their parents."

- K.K., a twelfth grader, creates a MySpace group named S.A.S.H. for discussing a fellow student, Shay H. (The name allegedly stands either for "Students Against Sluts Herpes" or "Students Against Shay's Herpes.)" She invites approximately 100 MySpace friends, including numerous other students, to join the group. Another student, R.P., posts a photograph of Shay H., altered to make it appear as though she has red dots on her face. A caption near her pelvic region reads, ""Warning: Enter at your own risk." After Shay H's father calls R.P. and expresses anger, K.K. attempts to delete the group but is unable to, and instead renames it "Students Against Angry People."

Bernstein v. U.S. Dept. of Justice

176 F. 3d 1132 (9th Cir.),
withdrawn and reh'g en banc granted, 192 F.3d 1308 (9th Cir. 1999)

Fletcher, Circuit Judge: ...

Background

A. Facts and Procedural History

Bernstein is currently a professor in the Department of Mathematics, Statistics, and Computer Science at the University of Illinois at Chicago. As a doctoral candidate at the University of California, Berkeley, he developed an encryption method – "a zero-delay private-key stream encryptor based upon a one-way hash function" that he dubbed "Snuf-

[*] [Ed: Presumably short for "Douglas High School."]

fle." Bernstein described his method in two ways: in a paper containing analysis and mathematical equations (the "Paper") and in two computer programs written in "C," a high-level computer programming language ("Source Code"). Bernstein later wrote a set of instructions in English (the "Instructions") explaining how to program a computer to encrypt and decrypt data utilizing a one-way hash function, essentially translating verbatim his Source Code into prose form.

Seeking to present his work on Snuffle within the academic and scientific communities, Bernstein asked the State Department whether he needed a license to publish Snuffle in any of its various forms. The State Department responded that Snuffle was a munition under the [Export Administration Regulations ("EAR") administered by the Bureau of Export Administration ("BXA")], and that Bernstein would need a license to "export" the Paper, the Source Code, or the Instructions.

There followed a protracted and unproductive series of letter communications between Bernstein and the government, wherein Bernstein unsuccessfully attempted to determine the scope and application of the export regulations to Snuffle. [Bernstein sued, and the District Court held that the EAR constituted a constitutionally impermissible prior restraint on speech.]

B. Overview of Cryptography

Cryptography is the science of secret writing, a science that has roots stretching back hundreds, and perhaps thousands, of years. For much of its history, cryptography has been the jealously guarded province of governments and militaries. In the past twenty years, however, the science has blossomed in the civilian sphere, driven on the one hand by dramatic theoretical innovations within the field, and on the other by the needs of modern communication and information technologies. As a result, cryptography has become a dynamic academic discipline within applied mathematics. It is the cryptographer's primary task to find secure methods to encrypt messages, making them unintelligible to all except the intended recipients:

> Encryption basically involves running a readable message known as "plaintext" through a computer program that translates the message according to an equation or algorithm into unreadable "ciphertext." Decryption is the translation back to plaintext when the message is received by someone with an appropriate "key."

Bernstein [*v. U.S. Department of State*, 974 F. Supp. 1288, 1292 (N.D. Cal. 1997)]. The applications of encryption, however, are not limited to ensuring secrecy; encryption can also be employed to ensure data integrity, authenticate users, and facilitate nonrepudiation (e.g., linking a specific message to a specific sender).

It is, of course, encryption's secrecy applications that concern the government. The interception and deciphering of foreign communications has long played an important part in our nation's national security efforts. In the words of a high-ranking State Department official:

> Policies concerning the export control of cryptographic products are based on the fact that the proliferation of such products will make it easier for foreign intelligence targets to deny the United States Government access to information vital to national security interests. Cryptographic products and software have military and intelligence applications. As demonstrated throughout history, encryption has been used to conceal foreign military communications, on the battlefield, aboard ships and submarines, or in other military settings. Encryption is also used to conceal other foreign

> communications that have foreign policy and national security significance for the United States. For example, encryption can be used to conceal communications of terrorists, drug smugglers, or others intent on taking hostile action against U.S. facilities, personnel, or security interests.

Lowell Decl. at 4. As increasingly sophisticated and secure encryption methods are developed, the government's interest in halting or slowing the proliferation of such methods has grown keen. The EAR regulations at issue in this appeal evidence this interest.

C. The EAR regulations

The EAR contain specific regulations to control the export of encryption software, expressly including computer source code. [The "export" of encryption software was defined] to preclude the use of the internet and other global mediums if such publication would allow passive or active access by a foreign national within the United States or anyone outside the United States. 15 C.F.R. § 734.2(b)(9)(B)(ii). ...

If encryption software falls within the ambit of the relevant EAR provisions, the "export" of such software requires a prepublication license. When a prepublication license is requested, the relevant agencies undertake a "case-by-case" analysis to determine if the export is "consistent with U.S. national security and foreign policy interests." 15 C.F.R. § 742.15(b). ...

Discussion

I. Prior Restraint

The parties and *amici* urge a number of theories on us. We limit our attention here, for the most part, to only one: whether the EAR restrictions on the export of encryption software in source code form constitute a prior restraint in violation of the First Amendment. We review *de novo* the district court's affirmative answer to this question.

It is axiomatic that "prior restraints on speech and publication are the most serious and least tolerable infringement on First Amendment rights." *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976). Indeed, the Supreme Court has opined that "it is the chief purpose of the [First Amendment] guaranty to prevent previous restraints upon publication." *Near v. Minnesota*, 283 U.S. 697, 713 (1931). Accordingly, "[a]ny prior restraint on expression comes . . . with a 'heavy presumption' against its constitutional validity." *Organization for a Better Austin v. Keefe,* 402 U.S. 415, 419 (1971). ...

A. Is Bernstein entitled to bring a facial attack?

A licensing regime is always subject to facial challenge as a prior restraint where it "gives a government official or agency substantial power to discriminate based on the content or viewpoint of speech by suppressing disfavored speech or disliked speakers," and has "a close enough nexus to expression, or to conduct commonly associated with expression, to pose a real and substantial threat of . . . censorship risks." *Id.* at 759.

The EAR regulations at issue plainly satisfy the first requirement – "the determination of who may speak and who may not is left to the unbridled discretion of a government official." *Id.* at 763. BXA administrators are empowered to deny licenses whenever export might be inconsistent with "U.S. national security and foreign policy interests." 15 C.F.R. § 742.15(b). No more specific guidance is provided. Obviously, this constraint on official discretion is little better than no constraint at all. ...

The more difficult issue arises in relation to the second requirement – that the challenged regulations exhibit "a close enough nexus to expression." We are called on to determine whether encryption source code is expression for First Amendment purposes.

We begin by explaining what source code is. "Source code," at least as currently understood by computer programmers, refers to the text of a program written in a "high-level" programming language, such as "PASCAL" or "C." The distinguishing feature of source code is that it is meant to be read and understood by humans and that it can be used to express an idea or a method. A computer, in fact, can make no direct use of source code until it has been translated ("compiled") into a "low-level" or "machine" language, resulting in computer-executable "object code." That source code is meant for human eyes and understanding, however, does not mean that an untutored lay-person can understand it. Because source code is destined for the maw of an automated, ruthlessly literal translator – the compiler – a programmer must follow stringent grammatical, syntactical, formatting, and punctuation conventions. As a result, only those trained in programming can easily understand source code.[11]

Also important for our purposes is an understanding of how source code is used in the field of cryptography. Bernstein has submitted numerous declarations from cryptog-

---

[11] It must be emphasized, however, that source code is merely text, albeit text that conforms to stringent formatting and punctuation requirements. For example, the following is an excerpt from Bernstein's Snuffle source code:

```
for (; ;)
  (
  uch = gtchr( );
  if (!(n & 31))
    (
    for (i = 0; i<64; i + +)
    l[ctr[i]] = k[i] + h[n - 64 + i]
    Hash512 (wm, wl, level, 8);
    )
```

As source code goes, Snuffle is quite compact; the entirety of the Snuffle source code occupies fewer than four printed pages.

raphers and computer programmers explaining that cryptographic ideas and algorithms are conveniently expressed in source code.[12]

That this should be so is, on reflection, not surprising. As noted earlier, the chief task for cryptographers is the development of secure methods of encryption. While the articulation of such a system in layman's English or in general mathematical terms may be useful, the devil is, at least for cryptographers, often in the algorithmic details. By utilizing source code, a cryptographer can express algorithmic ideas with precision and methodological rigor that is otherwise difficult to achieve. This has the added benefit of facilitating peer review – by compiling the source code, a cryptographer can create a working model subject to rigorous security tests. The need for precisely articulated hypotheses and formal empirical testing, of course, is not unique to the science of cryptography; it appears, however, that in this field, source code is the preferred means to these ends.

Thus, cryptographers use source code to express their scientific ideas in much the same way that mathematicians use equations or economists use graphs. Of course, both mathematical equations and graphs are used in other fields for many purposes, not all of which are expressive. But mathematicians and economists have adopted these modes of expression in order to facilitate the precise and rigorous expression of complex scientific ideas. Similarly, the undisputed record here makes it clear that cryptographers utilize source code in the same fashion.

In light of these considerations, we conclude that encryption software, in its source code form[15] and as employed by those in the field of cryptography, must be viewed as expressive for First Amendment purposes, and thus is entitled to the protections of the prior

---

[12] Source code's power to convey algorithmic information is illustrated by the declaration of MIT Professor Harold Abelson:

> The square root of a number X is the number Y such that Y times Y equals X. This is declarative knowledge. It tells us something about square roots. But it doesn't tell us how to find a square root. In contrast, consider the following ancient algorithm, attributed to Heron of Alexandria, for approximating square roots:
>
> To approximate the square root of a positive number X,
>
> – Make a guess for the square root of X.
>
> – Compute an improved guess as the average of the guess and X divided by the guess.
>
> – Keep improving the guess until it is good enough.
>
> Heron's method doesn't say anything about what square roots are, but it does say how to approximate them. This is a piece of imperative "how to" knowledge.
>
> Computer science is in the business of formalizing imperative knowledge – developing formal notations and ways to reason and talk about methodology. Here is Heron's method formalized as a procedure in the notation of the Lisp computer language:

```
(define (sqrtx)
  (define (good-enough? guess)
    (<(abs ( - (square guess) x)) tolerance))
  (define (improve guess)
    (average guess (/ × guess)))
  (define (try guess)
    (if (good-enough? guess)
    guess
    (try (improve guess))))
  (try 1))
```

[15] We express no opinion regarding whether object code manifests a "close enough nexus to expression" to warrant application of the prior restraint doctrine. Bernstein's Snuffle did not involve object code, nor does the record contain any information regarding expressive uses of object code in the field of cryptography.

restraint doctrine. If the government required that mathematicians obtain a prepublication license prior to publishing material that included mathematical equations, we have no doubt that such a regime would be subject to scrutiny as a prior restraint. The availability of alternate means of expression, moreover, does not diminish the censorial power of such a restraint – that Adam Smith wrote *Wealth of Nations* without resorting to equations or graphs surely would not justify governmental prepublication review of economics literature that contain these modes of expression.

The government, in fact, does not seriously dispute that source code is used by cryptographers for expressive purposes. Rather, the government maintains that source code is different from other forms of expression (such as blueprints, recipes, and "how-to" manuals) because it can be used to control directly the operation of a computer without conveying information to the user. In the government's view, by targeting this unique functional aspect of source code, rather than the content of the ideas that may be expressed therein, the export regulations manage to skirt entirely the concerns of the First Amendment. This argument is flawed for at least two reasons.

First, it is not at all obvious that the government's view reflects a proper understanding of source code. As noted earlier, the distinguishing feature of source code is that it is meant to be read and understood by humans, and that it *cannot* be used to control directly the functioning of a computer. While source code, when properly prepared, can be easily compiled into object code by a user, ignoring the distinction between source and object code obscures the important fact that source code is not meant solely for the computer, but is rather written in a language intended also for human analysis and understanding.

Second, and more importantly, the government's argument, distilled to its essence, suggests that even one drop of "direct functionality" overwhelms any constitutional protections that expression might otherwise enjoy. This cannot be so. The distinction urged on us by the government would prove too much in this era of rapidly evolving computer capabilities. The fact that computers will soon be able to respond directly to spoken commands, for example, should not confer on the government the unfettered power to impose prior restraints on speech in an effort to control its "functional" aspects. The First Amendment is concerned with expression, and we reject the notion that the admixture of functionality necessarily puts expression beyond the protections of the Constitution. ...

[The court held that the export restrictions were a constitutionally impermissible prior restraint on speech.]

Nelson, Circuit Judge, Dissenting: ...

The basic error which sets the majority and the district court adrift is the failure to fully recognize that the basic function of encryption source code is to act as a method of controlling computers. As defined in the EAR regulations, encryption source code is "[a] precise set of operating instructions to a computer, that when compiled, allows for the execution of an encryption function on a computer." 15 C.F.R. pt. 722. Software engineers generally do not create software in object code-the series of binary digits (1's and 0's) – which tells a computer what to do because it would be enormously difficult, cumbersome and time-consuming. Instead, software engineers use high-level computer programming languages such as "C" or "Basic" to create source code as a shorthand method for telling the computer to perform a desired function. In this respect, lines of source code are the building blocks or the tools used to create an encryption machine. Encryption source code, once compiled, works to make computer communication and transactions secret; it

creates a lockbox of sorts around a message that can only be unlocked by someone with a key. It is the function or task that encryption source code performs which creates its value in most cases. This functional aspect of encryption source code contains no expression; it is merely the tool used to build the encryption machine. ...

This is not to say that this very same source code is not used expressively in some cases. Academics, such as Bernstein, seek to convey and discuss their ideas concerning computer encryption. As noted by the majority, Bernstein must actually use his source code textually in order to discuss or teach cryptology. In such circumstances, source code serves to express Bernstein's scientific methods and ideas.

While it is conceptually difficult to categorize encryption source code under our First Amendment framework, I am still inevitably led to conclude that encryption source code is more like conduct than speech. Encryption source code is a building tool. Academics and computer programmers can convey this source code to each other in order to reveal the encryption machine they have built. But, the ultimate purpose of encryption code is, as its name suggests, to perform the function of encrypting messages. Thus, while encryption source code may occasionally be used in an expressive manner, it is inherently a functional device. ...

The activity or conduct at issue here is the export of encryption source code. As I noted above, the basic nature of encryption source code lies in its functional capacity as a method to build an encryption device. Export of encryption source code is not conduct commonly associated with expression. Rather, it is conduct that is normally associated with providing other persons with the means to make their computer messages secret. The overwhelming majority of people do not want to talk about the source code and are not interested in any recondite message that may be contained in encryption source code. Only a few people can actually understand what a line of source code would direct a computer to do. Most people simply want to *use* the encryption source code to protect their computer communications. Export of encryption source code simply does not fall within the bounds of conduct commonly associated with expression such as picketing or handbilling. ...

[Following this decision, the Ninth Circuit granted rehearing *en banc*. While the rehearing was pending, the government exempted "publicly available encryption source code" from most of the EAR's restrictions, *see* 15 C.F.R. § 740.13(e), mooting the case. The export control laws continue to be enforced against other computer products: the Xbox.com website terms of service, for example, require users to agree to comply with export controls.]

Questions

1. How did computer software end up on the export control list along with surface-to-air missiles? How does the Internet make this a harder case?

2. Who has the clearer understanding of encryption software, the majority or the dissent?

3. How does the the First Amendment apply to object code?

4. Programs can be used not just to protect secrets but to discover them. There is a thriving grey market in "exploits": short programs that take advantage of security vulnerabilities in commonly-used software to let an attacker take control of a computer. Secrecy is key, because once an exploit is known, the company whose software it targets can fix the vulnerability. Some of the biggest exploit buyers are governments—including the United States government—looking to spy on each other, or own their own citizens. Some critics

think that the sale of exploits should be criminalized. But others argue that they are protected by the First Amendment. Who is right? Would it make a difference if the defendant sold only a plain-English description of a security vulnerability, but did not include the code to exploit it?

5. *Bernstein* deals with software exports; what about software imports? Consider the following not-entirely-hypothetical:

> The International Trade Commission has the power to prohibit "the importation into the United States … of articles that … infringe a … United States patent." 19 U.S.C. § 1337 (a)(1)(B). The Scrivello Corporation holds a patent on a particular style of dental braces that are customized to the wearer's mouth. A competitor, Szell Dental, creates digital models of the braces in Pakistan, then transmits the models over the Internet to a factory in the United States, where it manufactures the braces using a 3D printer.

Has Szell "imported" infringing "articles?"

6. Federal law imposes record-keeping requirements on firearm sales, prohibits felons from possessing firearms, and strictly limits private ownership of automatic weapons. Are these rules sustainable now that it is possible to manufacture a crude but usable handgun using a 3D printer? The Second Amendment protects "the right of the people to keep and bear Arms." Does it also protect the right to keep and bear digital models of firearms? What about a right to keep and bear exploits?

Note on the Press

The First Amendment protects both "the freedom of speech" and "of the press." Lawyers and scholars are divided on whether this second clause adds anything to the first. Some believe that the Constitution enshrines special protections for the media—especially the news media—because of their central role in democracy. Others believe that the Constitution values all speakers equally, amateurs as well as professionals, as long as they are engaged in protected "speech."

The question has a special urgency online. Increasingly, bloggers and independent activists are invoking laws originally written for the benefit of reporters and institutional media. For example, "media shield" laws protect reporters from being required to identify their confidential sources or turn over their unpublished files. Although forty-nine states have some kind of media shield protections, the details of who and what are covered, and when, vary significantly.[*] As a concrete example, here is California's:

> A publisher, editor, reporter, or other person connected with or employed upon a newspaper, magazine, or other periodical publication, or by a press association or wire service … cannot be adjudged in contempt by a judicial, legislative, administrative body, or any other body having the power to issue subpoenas, for refusing to disclose … the source of any information procured while so connected or employed for publication in a newspaper, magazine or other periodical publication, or for refusing to disclose any unpublished

[*] The Reporters Committee for Freedom of the Press has a detailed state-by-state survey of press shield laws and caselaw at `http://www.rcfp.org/reporters-privilege`. *See also U.S. v. Sterling*, 724 F.3d 482 (4th Cir. 2013) (holding 2–1 that there is no federal privilege against naming confidential sources and compelling *New York Times* reporter James Risen to say who told him about a classified C.I.A. operation to slow down Iran's nuclear weapons program).

> information obtained or prepared in gathering, receiving or processing of information for communication to the public.

CAL. EVID. CODE § 1070(a). A similar provision applies to "a radio or television news reporter." *Id.* § 1070(b). Do those statutory terms include Apple Insider, a website devoted to rumors and leaks about forthcoming Apple products? Yes, said a California court in *O'Grady v. Superior Court,* 44 Cal. Rptr. 3d 72, 99 (2006), writing that "the open and deliberate publication on a news-oriented Web site of news gathered for that purpose by the site's operators" was "conceptually indistinguishable from publishing a newspaper." Compare *Too Much Media, LLC, v. Hale*, 20 A.3d 364, 367 (N.J. 2011), which refused to apply New Jersey's shield law to "a self- described journalist who posted comments on an Internet message board." It compared her posts to "a pamphlet full of unfiltered, unscreened letters to the editor submitted for publication." *Id.* at 379.

Similarly, courts have been willing to allow news media to publish stories even when some of the information in those stories was obtained illegally. *New York Times Co. v. United States*, 403 U.S. 713 (1971) held that an order forbidding the New York Times from publishing the "Pentagon Papers" (a secret Defense Department study documenting the United States's military involvement in Vietnam) violated the First Amendment as an unconstitutional prior restraint. *Barnicki v. Vopper*, 532 U.S. 514 (2001) held that a radio commentator who was given a tape recording of two union officials discussing potentially violent negotiating tactics could play it on the air, because he "played no part in the illegal interception" and because "the subject matter of the conversation was a matter of public concern.." *Id.* at 525.

Other laws more clearly protect speakers in general. So-called "anti-SLAPP statutes" give defendants a chance to obtain early dismissal of lawsuits designed to chill free speech. ("SLAPP" is an acronym for Strategic Lawsuit Against Public Participation). Indiana, for example, allows defendants to file a motion to dismiss on the basis that "the act upon which the claim [against them] is based is a lawful act in furtherance of the person's right of petition or free speech." IND. CODE § 34-7-7-9(d). All other discovery is stayed, *id.* § 34-7-7-6, and the court must act on the motion expeditiously, *id* § 34-7-7-9(a)(2). In essence, the statute changes the usual sequence of civil case management so that the defendant can litigate her First Amendment arguments first without the expense and hassle of discovery. If she prevails, she is entitled to her reasonable attorneys' fees. *Id.* § 34-7-7-7. (Why?) For example, in *Gilbert v. Skyes*, 147 Cal. App. 4th 13 (2007), the court dismissed a plastic surgeon's defamation claim against a former patient. It held that a "slight discrepancy" in before-and-after photos at her website, `http://www.mysurgerynightmare.com`, did not make them false, and that her statement "I didn't need procedures and I had no idea what I was really getting myself into" was not injuriously false.

Questions

1. If you were drafting a press shield law for the digital age, what would it say? What facts would you want to know about a self-described "citizen journalist" to decide whether to let him or her refuse to name a source?

2. Should media shield laws have a carve-out for national-security information, like the NSA surveillance documents leaked by Edward Snowden? Or is the rationale for such laws even stronger with government secrets? Should the answer depend on whether the leaks are to established journalists like Glenn Greenwald at *The Guardian* and Barton Gellman at the *Washington Post* (to whom Snowden released thousands of NSA documents) or to non-mainstream outlets like WikiLeaks (to whom Chelsea Manning released

250,000 classified State Department cables)? Should the answer depend on how the law treats leakers and whistleblowers themselves?

3. Does the *Bartnicki* rationale also apply to a blogger who comes into possession of a video, shot by a trespasser, showing conditions inside a poultry plant? Or is there something about the institutional press that makes it more likely to use this privilege for the broader social good?

4. Are anti-SLAPP statutes a sensible protection for free speech, or an unnecessary piece of First Amendment exceptionalism? If the anti-SLAPP procedures are so good, why not make them available in all cases?

5. More and more Americans get their news online, frequently through aggregator sites that link to stories elsewhere do little of their own reporting, like the Huffington Post. Newspaper advertising and circulation are down significantly. What will happen to news reporting if traditional offline news outlets disappear entirely? Is the Internet the source of this problem, or the solution?

Blu-Ray Problem

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. The 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."[*] 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. Dozens of users reposted the number in threads all across the DVD

[*] For more on this provision, see *infra* Chapter 7.

Technical Forum. In addition, a user with the Forum username DVD Monkey considered 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?). ...

If you were advising the AACS LA, what actions would you suggest? Can the AACS-LA put the monkeys back in the barrel, or have the DVD Technical Forum's users made a monkey out of Blu-Ray security?

---

* The image is *Mnemonic MonKey Pirate* by ApeLad, posted to Flickr at http://www.flickr.com/photos/apelad/487654055/ and is available under a Creative Commons Attribution Noncommercial 2.0 license. The full license details are available at http://creativecommons.org/licenses/by-nc/2.0/deed.en.

B. Harmful Speech

Concluding that something is "speech" does not end the First Amendment inquiry. Some restrictions of speech are permissible; many of those restrictions are related to the harm that the speech causes. The materials in this section consider four kinds of harm that speech could cause: to the victim's reputation, sense of safety, privacy, and emotions. An early generation of theorists believed that these restrictions were either unenforceable or unnecessary on the Internet. They argued that online speech could and should be utterly uninhibited. As you read the following materials, ask what this view gets right and what it gets wrong.

DANAH BOYD, IT'S COMPLICATED: THE SOCIAL LIVES OF NETWORKED TEENS 10–13 (2014)

To understand what is new and what is not, it's important to understand how technology introduces new social possibilities and how these challenge assumptions people have about everyday interactions. The design and architecture of environments enable certain types of interaction to occur. Round tables with chairs make chatting with someone easier than classroom-style seating. Even though students can twist around and talk to the person behind them, a typical classroom is designed to encourage everyone to face the teacher. The particular properties or characteristics of an environment can be understood as *affordances* because they make possible – and, in some cases, are used to encourage – certain types of practices, even if they do not determine what practices will unfold. Understanding the affordances of a particular technology or space is important because it sheds light on what people can leverage or resist in achieving their goals. For example, the affordances of a thick window allow people to see each other without being able to hear each other. To communicate in spite of the window, they may pantomime, hold up signs with written messages, or break the glass. The window's affordances don't predict how people will communicate, but they do shape the situation nonetheless.

Because technology is involved, networked publics have different characteristics than traditional physical public spaces. Four affordances, in particular, shape many of the mediated environments that are created by social media. Although these affordances are not in and of themselves new, their relation to one another because of networked publics creates new opportunities and challenges. They are:

- persistence: the durability of online expressions and content;
- visibility: the potential audience who can bear witness;
- spreadability: the ease with which content can be shared;
- and searchability: the ability to find content.

Content shared through social media often sticks around because technologies are designed to enable *persistence*. The fact that content often persists has significant implications. Such content enables interactions to take place over time in an asynchronous fashion. Alice may write to Bob at midnight while Bob is sound asleep; but when Bob wakes up in the morning or comes back from summer camp three weeks later, that message will still be there waiting for him, even if Alice had forgotten about it. Persistence means that conversations conducted through social media are far from ephemeral; they endure. Persistence enables different kinds of interactions than the ephemerality of a park. Alice's message doesn't expire when Bob reads it, and Bob can keep that message for decades. What persistence also means, then, is that those using social media are often "on the record" to an unprecedented degree.

Through social media, people can easily share with broad audiences and access content from greater distances, which increases the potential *visibility* of any particular message. More often than not, what people put up online using social media is widely accessible because most systems are designed such that sharing with broader or more public audiences is the default. Many popular systems require users to take active steps to limit the visibility of any particular piece of shared content. This is quite different from physical spaces, where people must make a concerted effort to make content visible to sizable audiences. In networked publics, interactions are often public by default, private through effort.

Social media is often designed to help people spread information, whether by explicitly or implicitly encouraging the sharing of links, providing reblogging or favoriting tools that repost images or texts, or by making it easy to copy and paste content from one place to another. Thus, much of what people post online is easily *spreadable* with the click of a few keystrokes.[9] Some systems provide simple buttons to "forward," "repost," or "share" content to articulated or curated lists. Even when these tools aren't built into the system, content can often be easily downloaded or duplicated and then forwarded along. The ease with which everyday people can share media online is unrivaled, which can be both powerful and problematic. Spreadability can be leveraged to rally people for a political cause or to spread rumors.

Last, since the rise of search engines, people's communications are also often *searchable*. My mother would have loved to scream, "Find!" and see where my friends and I were hanging out and what we were talking about. Now, any inquisitive onlooker can query databases and uncover countless messages written by and about others. Even messages that were crafted to be publicly accessible were not necessarily posted with the thought that they would reappear through a search engine. Search engines make it easy to surface esoteric interactions. These tools are often designed to eliminate contextual cues, increasing the likelihood that searchers will take what they find out of context.

None of the capabilities enabled by social media are new. The letters my grandparents wrote during their courtship were persistent. Messages printed in the school newspaper or written on bathroom walls have long been visible. Gossip and rumors have historically spread like wildfire through word of mouth. And although search engines certainly make inquiries more efficient, the practice of asking after others is not new, even if search engines mean that no one else knows. What is new is the way in which social media alters and amplifies social situations by offering technical features that people can use to engage in these well-established practices.

As people use these different tools, they help create new social dynamics. For example, teens "stalk" one another by searching for highly visible, persistent data about people they find interesting. "Drama" starts when teens increase the visibility of gossip by spreading it as fast as possible through networked publics. And teens seek attention by exploiting searchability, spreadability, and persistence to maximize the visibility of their garage band's YouTube video. The particular practices that emerge as teens use the tools around them create the impression that teen sociality is radically different even though the underlying motivations and social processes have not changed that much.

Questions

1. Is a handwritten letter persistent? Visible? Spreadable? Searchable? What about an email? A blog post?

2. How do these four affordances change the ways in which speech can inflict harms on listeners? On speakers? On third parties?

3. John Perry Barlow argues that online speech is different because the Internet is *all speech*. How does this play into his argument that governments should keep their hands off the Internet? Do boyd's claims support his argument, or undercut it?

Restatement (Second) of Torts [Privacy Torts]

§ 558 Elements [of Defamation] 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) [harm].

§ 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.

§ 568 Libel and Slander Distinguished

(1) Libel consists of the publication of defamatory matter by written or printed words, by its embodiment in physical form or by any other form of communication that has the potentially harmful qualities characteristic of written or printed words.

(2) Slander consists of the publication of defamatory matter by spoken words, transitory gestures or by any form of communication other than those stated in Subsection (1).

(3) The area of dissemination, the deliberate and premeditated character of its publication and the persistence of the defamation are factors to be considered in determining whether a publication is a libel rather than a slander.

§ 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.

cmt. b. The invasion may be by physical intrusion into a place in which the plaintiff has secluded himself, as when the defendant forces his way into the plaintiff's room in a hotel or insists over the plaintiff's objection in entering his home. It may also be by the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires. It may be by some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents. ...

cmt. c. The defendant is subject to liability under the rule stated in this Section only when he has intruded into a private place, or has otherwise invaded a private seclusion that the plaintiff has thrown about his person or affairs. Thus there is no liability for the examination of a public record concerning the plaintiff, or of documents that the plaintiff is required to keep and make available for public inspection. Nor is there liability for observing him or even taking his photograph

while he is walking on the public highway, since he is not then in seclusion, and his appearance is public and open to the public eye. Even in a public place, however, there may be some matters about the plaintiff, such as his underwear or lack of it, that are not exhibited to the public gaze; and there may still be invasion of privacy when there is intrusion upon these matters.

§ 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.

Pennsylvania Right of Publicity

Title 42, Pennsylvania Consolidated Statutes

§ 8316. Unauthorized use of name or likeness

(a) *Cause of action established.*–Any natural person whose name or likeness has commercial value and is used for any commercial or advertising purpose without the written consent of such natural person ... may bring an action to enjoin such unauthorized use and to recover damages for any loss or injury sustained by such use. ...

(c) *Repose.*–No action shall be commenced under this section more than 30 years after the death of such natural person. ...

(e) *Definitions.*–As used in this section, the following words and phrases shall have the meanings given to them in this subsection:

"Commercial or advertising purpose."

(1) Except as provided in paragraph (2), the term shall include the public use or holding out of a natural person's name or likeness:

(i) on or in connection with the offering for sale or sale of a product, merchandise, goods, services or businesses;

(ii) for the purpose of advertising or promoting products, merchandise, goods or services of a business; or

(iii) for the purpose of fundraising.

(2) The term shall not include the public use or holding out of a natural person's name or likeness in a communications medium when:

(i) the natural person appears as a member of the public and the natural person is not named or otherwise identified;

(ii) it is associated with a news report or news presentation having public interest;

(iii) it is an expressive work; ...

"*Expressive work.*" A literary, dramatic, fictional, historical, audiovisual or musical work regardless of the communications medium by which it is exhibited, displayed, performed or transmitted, other than when used or employed for a commercial or advertising purpose.

Questions

1. On May 12, 2009, Amanda Bonnen used Twitter to tweet:

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

Horizon Group Management, her former landlord, sued for defamation. Is Bonnen's 127-character tweet legally actionable? If Bonnen had told her friends in person about the mold in her apartment, rather than using Twitter, could there have been a lawsuit?

2. Some commentators have argued that the tort of defamation is outdated in the digital world and should be abolished. They claim that victims like Horizon can now take to the Internet to tell their side of the story, so they don't need legal remedies. Do you agree?

3. What does the intrusion on seclusion tort have to do with speech? Is there a First Amendment right to listen and observe as well as to speak? If so, what work are the concepts of "public place" and "private place" doing in defining the contours of the tort? Is it legal to videotape interactions with the police? To take photographs up the skirts of women seated on the subway? To fly a drone outside a neighbor's window?

4. What is the difference between "publicity given to private life" and the "right of publicity?"

Gawker Media, LLC v. Bollea

129 So. 3d 1196 (Dist. Ct. App. Fla. 2014)

Black, Judge:

Terry Bollea sought to enjoin Gawker Media, LLC, from publishing and otherwise distributing the written report about his extramarital affair that includes video excerpts from the sexual encounter. The circuit court granted Mr. Bollea's motion for temporary injunction, though it did not articulate the reasons for doing so. ... Because the temporary injunction is an unconstitutional prior restraint under the First Amendment, we reverse.

I. Background

In 2006, Mr. Bollea engaged in extramarital sexual relations with a woman in her home. Allegedly without Mr. Bollea's consent or knowledge, the sexual encounter was videotaped. On or about October 4, 2012, Gawker Media posted a written report about the extramarital affair on its website, including excerpts of the videotaped sexual encounter ("Sex Tape"). Mr. Bollea maintains that he never consented to the Sex Tape's release or publication. Gawker Media maintains that it was not responsible for creating the Sex Tape and that it received a copy of the Sex Tape from an anonymous source for no compensation.

[Bollea filed a federal action, then voluntarily dismissed it after the court denied his motion for a preliminary injunction.] That same day, Mr. Bollea filed an amended complaint in state circuit court, asserting essentially the same claims that he asserted in federal court. Thereafter and as he did in federal court, Mr. Bollea filed a motion for temporary injunction seeking to enjoin Gawker Media ... from publishing and otherwise distributing the video excerpts from the sexual encounter and complementary written report. Following a hearing, the circuit court issued an order on April 25, 2012, granting the motion for temporary injunction. The court did not make any findings at the hearing or in its written order to support its decision. On May 15, 2013, this court stayed the order granting the motion for temporary injunction pending the resolution of this appeal.

II. Applicable Standards

The primary purpose of a temporary injunction is to preserve the status quo while the merits of the underlying dispute are litigated. In the context of the media, the status

quo is to publish news promptly that editors decide to publish. A restraining order disturbs the status quo and impinges on the exercise of editorial discretion. A temporary injunction is an extraordinary remedy that should be granted sparingly and only after the moving party has alleged and proved facts entitling him to relief.

A temporary injunction aimed at speech, as it is here, is a classic example of prior restraint on speech triggering First Amendment concerns, and as such, it is prohibited in all but the most exceptional cases. Since "prior restraints on speech and publication are the most serious and least tolerable infringement on First Amendment rights," the moving party bears the "heavy burden" of establishing that there are no less extreme measures available to "mitigate the effects of the unrestrained . . . public[ation]" and that the restraint will indeed effectively accomplish its purpose. *Neb. Press Ass'n v. Stuart,* 427 U.S. 539, 558–59, 562 (1976). Furthermore, "[w]here . . . a direct prior restraint is imposed upon the reporting of news by the media, each passing day may constitute a separate and cognizable infringement of the First Amendment." *Neb. Press Ass'n v. Stuart,* 423 U.S. 1327, 1329 (Blackmun, Circuit Justice, 1975). ...

III. First Amendment

It is not clear from the hearing transcript, and certainly not from the order, why the circuit court granted the motion for temporary injunction. Based upon the few interjections the court made during the hearing, it appears that the court believed Mr. Bollea's right to privacy was insurmountable and that publishing the content at issue was otherwise impermissible because it was founded upon illegal actions.

A. Privacy

"[W]here matters of purely private significance are at issue, First Amendment protections are often less rigorous." Snyder v. Phelps, 131 S.Ct. 1207, 1215 (2011). On the other hand, "speech on matters of public concern . . . is at the heart of the First Amendment's protection." *Id.*

> Speech deals with matters of public concern when it can be fairly considered as relating to any matter of political, social, or other concern to the community, or when it is a subject of legitimate news interest; that is, a subject of general interest and of value and concern to the public. The arguably inappropriate or controversial character of a statement is irrelevant to the question whether it deals with a matter of public concern.

Id. at 1216. Mr. Bollea, better known by his ring name Hulk Hogan, enjoyed the spotlight as a professional wrestler, and he and his family were depicted in a reality television show detailing their personal lives. Mr. Bollea openly discussed an affair he had while married to Linda Bollea in his published autobiography and otherwise discussed his family, marriage, and sex life through various media outlets. Further, prior to the publication at issue in this appeal, there were numerous reports by various media outlets regarding the existence and dissemination of the Sex Tape, some including still shots therefrom. Despite Mr. Bollea's public persona, we do not suggest that every aspect of his private life is a subject of public concern. *See generally Post–Newsweek Stations Orlando, Inc. v. Guetzloe*, 968 So. 2d 608, 612 (Fla. 5th DCA 2007) (noting that appellant's status as a public figure does not mean that every aspect of his private life is of public concern but nonetheless holding that enjoining the broadcaster from publicly airing appellant's personal records and those of his family operated as an unconstitutional prior restraint under the First Amendment). However, the mere fact that the publication contains arguably inappropriate and otherwise sexually explicit content does not remove it from the realm of legitimate public interest. *See Fla. Star v. B.J.F.,* 491 U.S. 524, 525 (1989) (holding that

a news article about a rape was a matter of public concern and that the newspaper was not liable for the publication of the victim's identity obtained from a police report released by law enforcement in violation of a Florida statute); *Cape Publ'ns, Inc. v. Hitchner*, 549 So. 2d 1374, 1377 (Fla. 1989) (holding that confidential information regarding a child abuse trial was a matter of legitimate public concern and that thus the newspaper's publication of such did not violate privacy interests). It is clear that as a result of the public controversy surrounding the affair and the Sex Tape, exacerbated in part by Mr. Bollea himself,[5] the report and the related video excerpts address matters of public concern. *See Michaels v. Internet Entm't Grp., Inc.*, No. CV 98–0583 DDP (CWx), 1998 WL 882848, at *10 (C.D.Cal. Sept. 11, 1998) (*Michaels II*) ("[T]he private facts depicted in the [publication] ha[d] a substantial nexus to a matter of legitimate public interest," namely, a dispute over the dissemination of the sex tape, and the depiction of the sexual relations was "clearly part of the story."); *see also Jones v. Turner*, No. 94 Civ. 8603(PKL), 1995 WL 106111, at *21 (S.D.N.Y. Feb. 7, 1995) (holding that the preliminary injunction was unjustifiable where nude pictures were related to the accompanying article and the article itself was a matter of public concern). *But see City of San Diego, Cal. v. Roe*, 543 U.S. 77, 84 (2004) (holding that the sexually explicit acts of the government employee, depicted in a video, did not address a matter of public concern where the acts "did nothing to inform the public about any aspect of the [employing agency's] functioning or operation"); *Toffoloni v. LFP Publ'g Grp., LLC*, 572 F.3d 1201, 1213 (11th Cir. 2009) (holding that the publication of nude photographs of a female professional wrestler taken twenty years prior was not protected speech because their publication was not related to the content of the reporting, namely, her murder).

In support of his contention that the report and video excerpts do not qualify as matters of public concern, Mr. Bollea relies on *Michaels v.Internet Entertainment Group, Inc.*, 5 F. Supp. 2d 823(C.D.Cal. 1998) (*Michaels I*), in which the court enjoined the commercial distribution of an entire sex tape that infringed the plaintiffs' copyrights. However, the court in *Michaels I* found the use of the sex tape to be purely commercial in nature. Specifically, the copyrighted tape was sold via the internet to paying subscribers, and the internet company displayed short segments of the tape as a means of advertisement to increase the number of subscriptions. In contrast, Gawker Media has not attempted to sell the Sex Tape or any of the material creating the instant controversy, for that matter.[6] Rather, Gawker Media reported on Mr. Bollea's extramarital affair and complementary thereto posted excerpts from the video.

The court in *Michaels I* pointed out that although "[t]he plaintiffs are entitled to an injunction against uses of their names or likenesses to sell the [sex tape,] [t]he injunction may not reach the use of their names or likenesses to report or comment on matters

---

[5] We are hard-pressed to believe that Mr. Bollea truly desired the affair and Sex Tape to remain private or to otherwise be "swept under the rug." For example, in March 2012, Mr. Bollea called into TMZ Live, a celebrity and entertainment media outlet, and disclosed that he could not identify the woman in the Sex Tape because he had a number of "conquests" during the time it was filmed. Furthermore, in October 2012, Mr. Bollea appeared on The Howard Stern Show and professed that his good friend, Todd Alan Clem, known professionally as Bubba the Love Sponge, allowed Mr. Bollea to have sex with Mr. Clem's then-wife Heather Clem. Mr. Bollea was certainly not shy about disclosing the explicit details of another affair he had while married to Linda Bollea in his autobiography.

[6] We are aware that Gawker Media is likely to profit indirectly from publishing the report with video excerpts to the extent that it increases traffic to Gawker Media's website. However, this is distinguishable from selling the Sex Tape purely for commercial purposes.

of public interest." In accord with this conclusion, the court held in the companion case that the publication of a news report and brief excerpts of the sex tape was not an invasion of privacy and was protected speech. *Michaels II*, 1998 WL 882848, at *7, *10 (distinguishing the dissemination of an entire sex tape with the use of excerpts from the tape); *see also Bollea v. Gawker Media, LLC*, 913 F.Supp.2d 1325, 1331 n. 6 (M.D. Fla. 2012) ("[Gawker Media] did not simply post the entire [Sex Tape]—or substantial portions thereof, but rather posted a carefully edited excerpt consisting of less than two minutes of the thirty[-]minute video of which less than ten seconds depicted explicit sexual activity."). Here, the written report and video excerpts are linked to a matter of public concern—Mr. Bollea's extramarital affair and the video evidence of such—as there was ongoing public discussion about the affair and the Sex Tape, including by Mr. Bollea himself. Therefore, Mr. Bollea failed to meet the heavy burden to overcome the presumption that the temporary injunction is invalid as an unconstitutional prior restraint under the First Amendment. As such, it was within Gawker Media's editorial discretion to publish the written report and video excerpts.

B. Unlawful Interception

It appears that the circuit court may have been convinced by Mr. Bollea's argument that the speech at issue is not entitled to First Amendment protection because the Sex Tape was created in violation of the law.[7] However, there is no dispute that Gawker Media was not responsible for the creation of the Sex Tape. Nor has Mr. Bollea alleged that Gawker Media otherwise obtained it unlawfully. The Supreme Court in *Bartnicki* held that if a publisher lawfully obtains the information in question, the speech is protected by the First Amendment provided it is a matter of public concern, even if the source recorded it unlawfully. *see also N.Y. Times Co. v. United States,* 403 U.S. 713, 91 S.Ct. 2140, 29 L.Ed.2d 822 (1971) (holding that notwithstanding the fact that a third party had stolen the information, the press had a constitutional right to publish the Pentagon Papers because they were of public concern). As the speech in question here is indeed a matter of legitimate public concern, the holding in *Bartnicki* applies.[8] As such, the temporary injunction acts as an unconstitutional prior restraint on Gawker Media's protected speech. ...

V. Conclusion

The circuit court's order granting Mr. Bollea's motion for temporary injunction is reversed because it acts as an unconstitutional prior restraint under the First Amendment.

People v. Marquan M.

24 N.Y.3d 1 (2014)

Graffeo, Justice:

Defendant, a 16–year–old high school student, anonymously posted sexual information about fellow classmates on a publicly-accessible Internet website. He was criminally prosecuted for "cyberbullying" under a local law enacted by the Albany County Leg-

---

[7] Mr. Bollea cites to the offense of video voyeurism, section 810.145(2)(a), Florida Statutes (2006), and to the offense of interception and disclosure of electronic communications, section 934.03, Florida Statutes (2006), in support of his contention.

[8] This opinion should not be construed as making a ruling regarding whether or not the information itself was intercepted unlawfully by Gawker Media's source.

islature. We are asked to decide whether this cyberbullying statute comports with the Free Speech Clause of the First Amendment.

I ...

Elected officials in Albany County decided to tackle the problem of cyberbullying. They determined there was a need to criminalize such conduct because the "State Legislature ha[d] failed to address th[e] problem" of "non-physical bullying behaviors transmitted by electronic means." Local Law No. 11 [2010] of County of Albany § 1. In 2010, the Albany County Legislature adopted a new crime—the offense of cyberbullying—which was defined as

> "any act of communicating or causing a communication to be sent by mechanical or electronic means, including posting statements on the internet or through a computer or email network, disseminating embarrassing or sexually explicit photographs; disseminating private, personal, false or sexual information, or sending hate mail, with no legitimate private, personal, or public purpose, with the intent to harass, annoy, threaten, abuse, taunt, intimidate, torment, humiliate, or otherwise inflict significant emotional harm on another person."

The provision outlawed cyberbullying against "any minor or person" situated in the county. Knowingly engaging in this activity was deemed to be a misdemeanor offense punishable by up to one year in jail and a $1,000 fine. The statute, which included a severability clause, became effective in November 2010.

II

A month later, defendant Marquan M., a student attending Cohoes High School in Albany County, used the social networking website "Facebook" to create a page bearing the pseudonym "Cohoes Flame." He anonymously posted photographs of high-school classmates and other adolescents, with detailed descriptions of their alleged sexual practices and predilections, sexual partners and other types of personal information. The descriptive captions, which were vulgar and offensive, prompted responsive electronic messages that threatened the creator of the website with physical harm.

A police investigation revealed that defendant was the author of the Cohoes Flame postings. He admitted his involvement and was charged with cyberbullying under Albany County's local law. Defendant moved to dismiss, arguing that the statute violated his right to free speech under the First Amendment. ...

III

Defendant contends that Albany County's cyberbullying law violates the Free Speech Clause of the First Amendment because it is overbroad in that it includes a wide array of protected expression, and is unlawfully vague since it does not give fair notice to the public of the proscribed conduct. The County concedes that certain aspects of the cyberbullying law are invalid but maintains that those portions are severable, rendering the remainder of the act constitutional if construed in accordance with the legislative purpose of the enactment. Interpreted in this restrictive manner, the County asserts that the cyberbullying law covers only particular types of electronic communications containing information of a sexual nature pertaining to minors and only if the sender intends to inflict emotional harm on a child or children.

Under the Free Speech Clause of the First Amendment, the government generally "has no power to restrict expression because of its message, its ideas, its subject matter, or its content." *United States v. Stevens*, 559 U.S. 460, 468 (2010). Consequently, it is well

established that prohibitions of pure speech must be limited to communications that qualify as fighting words, true threats, incitement, obscenity, child pornography, fraud, defamation or statements integral to criminal conduct. Outside of such recognized categories, speech is presumptively protected and generally cannot be curtailed by the government.

Yet, the government unquestionably has a compelling interest in protecting children from harmful publications or materials. Cyberbullying is not conceptually immune from government regulation, so we may assume, for the purposes of this case, that the First Amendment permits the prohibition of cyberbullying directed at children, depending on how that activity is defined. Our task therefore is to determine whether the specific statutory language of the Albany County legislative enactment can comfortably coexist with the right to free speech.

Challenges to statutes under the Free Speech Clause are usually premised on the overbreadth and vagueness doctrines. A regulation of speech is overbroad if constitutionally-protected expression may be "chilled" by the provision because it facially prohibits a real and substantial amount of expression guarded by the First Amendment This type of facial challenge, which is restricted to cases implicating the First Amendment, requires a court to assess the wording of the statute—without reference to the defendant's conduct—to decide whether a substantial number of its applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep. A law that is overbroad cannot be validly applied against any individual. In contrast, a statute is seen by the courts as vague if it fails to give a citizen adequate notice of the nature of proscribed conduct, and permits arbitrary and discriminatory enforcement. Hence, the government has the burden of demonstrating that a regulation of speech is constitutionally permissible. ...

Based on the text of the statute at issue, it is evident that Albany County created a criminal prohibition of alarming breadth. The language of the local law embraces a wide array of applications that prohibit types of protected speech far beyond the cyberbullying of children. As written, the Albany County law in its broadest sense criminalizes "any act of communicating . . . by mechanical or electronic means . . . with no legitimate . . . personal . . . purpose, with the intent to harass [or] annoy . . . another person." On its face, the law covers communications aimed at adults, and fictitious or corporate entities, even though the county legislature justified passage of the provision based on the detrimental effects that cyberbullying has on school-aged children. The county law also lists particular examples of covered communications, such as "posting statements on the internet or through a computer or email network, disseminating embarrassing or sexually explicit photographs; disseminating private, personal, false or sexual information, or sending hate mail." But such methods of expression are not limited to instances of cyberbullying—the law includes every conceivable form of electronic communication, such as telephone conversations, a ham radio transmission or even a telegram. In addition, the provision pertains to electronic communications that are meant to "harass, annoy . . . taunt . . . [or] humiliate" any person or entity, not just those that are intended to "threaten, abuse . . . intimidate, torment . . . or otherwise inflict significant emotional harm on" a child. In considering the facial implications, it appears that the provision would criminalize a broad spectrum of speech outside the popular understanding of cyberbullying, including, for example: an email disclosing private information about a corporation or a telephone conversation meant to annoy an adult.

The County admits that the text of the statute is too broad and that certain aspects of its contents encroach on recognized areas of protected free speech. Because the law imposes a restriction on the content of protected speech, it is invalid unless the

County can demonstrate that it passes strict scrutiny—that is, unless it is justified by a compelling government interest and is narrowly drawn to serve that interest. For this reason, the County asks us to sever the offending portions and declare that the remainder of the law survives strict scrutiny. What remains, in the County's view, is a tightly circumscribed cyberbullying law that includes only three types of electronic communications sent with the intent to inflict emotional harm on a child: (1) sexually explicit photographs; (2) private or personal sexual information; and (3) false sexual information with no legitimate public, personal or private purpose.

It is true, as the County urges, that a court should strive to save a statute when confronted with a Free Speech challenge. But departure from a textual analysis is appropriate only if the statutory language is fairly susceptible to an interpretation that satisfies applicable First Amendment requirements. The doctrine of separation of governmental powers prevents a court from rewriting a legislative enactment through the creative use of a severability clause when the result is incompatible with the language of the statute. And special concerns arise in the First Amendment context—excessive judicial revision of an overbroad statute may lead to vagueness problems because the statutory language would signify one thing but, as a matter of judicial decision, would stand for something entirely different. Under those circumstances, persons of ordinary intelligence reading [the law] could not know what it actually meant.

We conclude that it is not a permissible use of judicial authority for us to employ the severance doctrine to the extent suggested by the County or the dissent. It is possible to sever the portion of the cyberbullying law that applies to adults and other entities because this would require a simple deletion of the phrase "or person" from the definition of the offense. But doing so would not cure all of the law's constitutional ills. As we have recently made clear, the First Amendment protects annoying and embarrassing speech, even if a child may be exposed to it, so those references would also need to be excised from the definitional section. And, the First Amendment forbids the government from deciding whether protected speech qualifies as "legitimate," as Albany County has attempted to do.[4]

It is undisputed that the Albany County statute was motivated by the laudable public purpose of shielding children from cyberbullying. The text of the cyberbullying law, however, does not adequately reflect an intent to restrict its reach to the three discrete types of electronic bullying of a sexual nature designed to cause emotional harm to children. Hence, to accept the County's proposed interpretation, we would need to significantly modify the applications of the county law, resulting in the amended scope bearing little resemblance to the actual language of the law. Such a judicial rewrite encroaches on the authority of the legislative body that crafted the provision and enters the realm of vagueness because any person who reads it would lack fair notice of what is legal and what constitutes a crime. Even if the First Amendment allows a cyberbullying statute of the limited nature proposed by Albany County, the local law here was not drafted in that manner. Albany County therefore has not met its burden of proving that the restrictions on speech contained in its cyberbullying law survive strict scrutiny.

---

[4] Contrary to the dissent's position, *Shack* and *Stuart* are distinguishable because they addressed statutes that criminalized conduct—repeated telephone harassment and stalking—without regard to the content of any communication. Here, however, the Albany County law facially allows law enforcement officials to charge a crime based on the communicative message that the accused intends to convey, as evidenced by the fact that defendant was prosecuted because of the offensive words he wrote on Facebook.

There is undoubtedly general consensus that defendant's Facebook communications were repulsive and harmful to the subjects of his rants, and potentially created a risk of physical or emotional injury based on the private nature of the comments. He identified specific adolescents with photographs, described their purported sexual practices and posted the information on a website accessible world-wide. Unlike traditional bullying, which usually takes place by a face-to-face encounter, defendant used the advantages of the Internet to attack his victims from a safe distance, 24 hours a day, while cloaked in anonymity. Although the First Amendment may not give defendant the right to engage in these activities, the text of Albany County's law envelops far more than acts of cyberbullying against children by criminalizing a variety of constitutionally-protected modes of expression. We therefore hold that Albany County's Local Law No. 11 of 2010—as drafted—is overbroad and facially invalid under the Free Speech Clause of the First Amendment. ...

Smith, Justice, dissenting:

Albany County has conceded that certain provisions of its Cyber–Bullying law are invalid. It seems to me that those provisions can be readily severed from the rest of the legislation and that what remains can, without any strain on its language, be interpreted in a way that renders it constitutionally valid. ...

The County concedes that the words "embarrassing" and "hate mail" are vague and thus unenforceable. It argues, correctly I think, that these terms can be dealt with in the same way as the reference to "person" in the operative section: simply by crossing them out. Once these deletions are made, I see nothing in the law that renders it unconstitutional.

The majority, it seems, is troubled by two other aspects of the definition of "Cyber–Bullying": the requirement that the forbidden communications be made "with no legitimate private, personal, or public purpose"; and the series of verbs—"harass, annoy, threaten, abuse, taunt, intimidate, torment, humiliate"—that precedes the words "or otherwise." Neither requires us to invalidate the law.

I grant that the words "no legitimate . . . purpose" are not remarkable for their precision. We have twice held, however, that they are clear enough to withstand a constitutional challenge for vagueness. *People v. Shack*, 86 N.Y.2d 529, 533 (1995) (holding valid a prohibition on the making of a telephone call "with intent to harass, annoy, threaten or alarm another person . . . with no purpose of legitimate communication"); *People v. Stuart*, 100 N.Y.2d 412, 428 (2003) (holding valid an anti-stalking statute prohibiting a described course of conduct when engaged in "for no legitimate purpose"). We said in *Shack:*

> the phrase 'no purpose of legitimate communication' . . . notwithstanding its subjective quality, would be understood to mean the absence of expression of ideas or thoughts other than threats and/or intimidating or coercive utterances.

Similarly here, the phrase "no legitimate purpose" should be understood to mean the absence of expression of ideas or thoughts other than the mere abuse that the law proscribes.

It is true, as the majority says, that the criminal conduct at issue in *Shack* and *Stuart* was different from the conduct at issue here—but that does not make the words "no legitimate purpose" any more or less vague. The majority is also correct in saying that "the First Amendment forbids the government from deciding whether protected speech quali-

fies as 'legitimate' "but this begs the central question of what speech is "protected" and what is not. The Cyber–Bullying law prohibits a narrow category of valueless and harmful speech when the government proves, among other things, that the speaker had no legitimate purpose for engaging in it. The speech so prohibited is not protected speech.

As for the list of verbs beginning with "annoy" and ending with "humiliate," it is fair to read them, as the County urges, as "a non-exhaustive list of ways that the wrongdoer may formulate his or her intent to inflict emotional harm on the victim" In other words, the acts within the scope of the Cyber–Bullying law—disseminating sexually explicit photographs or private, personal, false or sexual information—are prohibited only where they are intended to "inflict significant emotional harm" on the victim, and the verbs merely serve as examples of ways in which significant emotional harm may be inflicted. That is not the only possible way to read the text of the law, but it is a perfectly reasonable way—indeed, the word "otherwise" seems to signal that the verbs preceding it are only illustrative. So read, the law does not prohibit conduct intended to harass, annoy, threaten or the like unless the actor specifically intended "significant emotional harm." I do not find such a prohibition to be unconstitutionally vague or overbroad. ...

Question

1. After *Marquan M*, would the following statute be constitutional?

> A minor commits a the offense of cyberbullying if the minor knowingly transmits or disseminates any electronic communication, including a visual depiction of himself or any other person in a state of nudity, to another minor with the knowledge or intent that the communication would coerce, intimidate, torment, harass or otherwise cause emotional distress to the other minor.

United States v. Petrovic*

701 F.3d 849 (8th Cir. 2012)

Riley, Chief Judge:

Jovica Petrovic was convicted of four counts of interstate stalking and two counts of interstate extortionate threat. The district court sentenced Petrovic to ninety-six months imprisonment. Petrovic appeals his convictions and sentence ... . We affirm.

I. Background ...

Petrovic and the victim, M.B., began a relationship in 2006, married in 2009, and later divorced. During their relationship, Petrovic resided in Florida and M.B. resided in Missouri, where she and her ex-husband, R.B., shared custody of their two young children. Petrovic and M.B. often met in Florida or Missouri, and M.B. occasionally allowed Petrovic to take pictures of her in the nude or performing various sex acts. M.B. also confided in Petrovic, revealing private and intimate information in text messages, such as the sexual abuse M.B. suffered as a young girl, her suicidal thoughts and tendencies, family secrets, and self-doubts about her fitness as a mother. Petrovic saved thousands of these text messages.

During their relationship, Petrovic also accumulated other potentially embarrassing information about M.B. In July 2009, M.B. attempted suicide at Petrovic's home after finding evidence leading her to believe Petrovic was having an extra-marital affair. After M.B. was taken to the hospital for treatment, Petrovic took pictures of the pool of blood that had formed on the floor. In December 2009, Petrovic took several trips to Missouri to

---

* [Ed: This case involves allegations of online harassment and threats of violence.]

see M.B. During these trips, Petrovic stayed at a local hotel and secretly filmed M.B. having sexual intercourse with him. Petrovic took steps to ensure that M.B. was identifiable in the videos. He refused to turn off the lights, removed the sheets from the bed, and directed M.B.'s face and exposed genitalia toward the concealed camera.

On December 28, 2009, M.B. informed Petrovic by text message that she was ending their relationship. In response, Petrovic sent M.B. text messages informing her that he had secretly recorded their recent sexual encounters and had saved all of the text messages M.B. previously sent him. Petrovic threatened to post this information on the internet so M.B.'s family could read the messages and see the videos, if M.B. did not continue their relationship. Petrovic stated he was not "blackmail[ing]" M.B. and was only saving the information for his own "protection," but told M.B. to "be smart." Petrovic informed M.B. she and her family could soon visit his new website, "www.[M.B.]slut. com." M.B. understood Petrovic intended to "ruin [her] life" if she did not "get back together with [Petrovic]," but M.B. nevertheless permanently ended the relationship.

Petrovic then began a campaign to carry out his threats. Over the course of the next few months, Petrovic mailed dozens of homemade postcards to addresses throughout M.B.'s community, including to M.B.'s workplace, M.B.'s family members, R.B.'s home, and local businesses like the neighborhood drugstore. The postcards typically portrayed a picture of a scantily clad M.B. along with abusive language (for example, "I am just a whore 4 sale") and directions to a website, "www.marriedto [M.B.].com." The postcards were viewed by M.B.'s children, other family members, and many acquaintances. News of the website spread throughout the community, and almost everyone M.B. knew became aware of the site.

The website was publicly accessible in March 2010. Petrovic reported his site was "huge," containing "20,000 or 30,000 pages" of material reflecting months of preparation by Petrovic, who began creating the site in August 2009. The site contained links to dozens of images of M.B. posing in the nude or engaging in sex acts with Petrovic, and included many from the tapes Petrovic secretly recorded. Visitors to the site could view scores of pictures of M.B.'s children and other family members by clicking on a link next to the pornographic material. Several photographs of M.B. performing a sex act with Petrovic were repeatedly and prominently displayed throughout the website, including on the site's home page. Petrovic also posted thousands of pages of the text messages M.B. had sent him. The messages were color-coded by speaker and organized chronologically, with the most private and embarrassing messages given special pages to increase readership. Petrovic posted the pictures of the blood from M.B.'s suicide attempt, further highlighting her suicidal thoughts and history. Private information about M.B. and her family was also revealed, including M.B.'s contact information and the social security numbers of her children. M.B. did not authorize Petrovic to release any of this information. After learning of the website, M.B. "had a breakdown" and "wanted to die."

Besides the website and postcards, Petrovic sent several packages containing enlarged photographs of M.B. engaging in various sex acts with Petrovic to M.B. at her work, to M.B.'s boss, to M.B.'s family members, and to R.B.'s home, where M.B.'s seven-year-old child viewed the pornographic material. Petrovic also repeatedly made harassing phone calls to M.B's workplace, and physically intimidated M.B. on several occasions — on one such occasion, pursuing M.B. in a rental van at a high rate of speed while M.B. was on her way home from work.

In June 2010, M.B.'s sister was able to have Petrovic's website shut down for a few days. On June 20, 2010, Petrovic relaunched the site and posted a message stating, "No-

body can stop me to publish this website" and offering to shut down the site if M.B. gave him his "furniture, what she stoled [sic] from me, the wedding and engagement ring, ... and $100,000." M.B. did not comply with Petrovic's demands, and the website remained operational. On July 19, 2010, Petrovic was arrested by United States Postal Inspectors.

On October 6, 2010, a grand jury indicted Petrovic with, among other charges, four counts of interstate stalking, in violation of 18 U.S.C. § 2261A(2)(A), and two counts of interstate extortionate threat, in violation of 18 U.S.C. § 875(d). Petrovic moved to dismiss the four stalking charges on the grounds the statute violated the First Amendment both facially and as applied to Petrovic. The district court denied this motion. ...

II. Discussion ...

Petrovic first argues 18 U.S.C. § 2261A(2)(A),[2] the interstate stalking statute, violates his right to freedom of speech under the First Amendment to the United States Constitution. Petrovic contends the statute is unconstitutional both facially and as applied to him. We review First Amendment challenges de novo.

"[W]hen 'speech' and 'nonspeech' elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms." *United States v. O'Brien*, 391 U.S. 367, 376 (1968). A governmental regulation satisfies this standard if (1) "it is within the constitutional power of the Government"; (2) "it furthers an important or substantial governmental interest"; (3) "the governmental interest is unrelated to the suppression of free expression"; and (4) "the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest." *Id.* at 377.

Petrovic contends § 2261A(2)(A) fails *O'Brien*'s four-pronged test in his case. However, we need not reach the merits of the *O'Brien* test if, as a preliminary matter, we determine the communications for which Petrovic was convicted under the statute are not protected by the First Amendment. Because we hold Petrovic's communications fall outside the First Amendment's protection, we do not reach the merits of the *O'Brien* test.

The First Amendment provides "Congress shall make no law ... abridging the freedom of speech." While it generally "means that government has no power to restrict expression because of its message, its ideas, its subject matter, or its content," *Ashcroft v. A.C.L.U.*, 535 U.S. 564, 573 (2002), certain "well-defined and narrowly limited classes of speech" permit content-based restrictions on speech, *United States v. Stevens,* 559 U.S. ___ (2010). One such category is "speech integral to criminal conduct." *Id.*; *see also Giboney v. Empire Storage & Ice Co.*, 336 U.S. 490, 498 (1949).

The jury convicted Petrovic of two counts of interstate extortionate threat in violation of 18 U.S.C. § 875(d) for his December 28, 2009 and June 20, 2010 communications. The communications for which Petrovic was convicted under § 2261A(2)(A) were integral to this criminal conduct as they constituted the means of carrying out his extortionate threats. *See Giboney*, 336 U.S. at 498, 501-02 (enjoining otherwise lawful picketing activities did not offend the First Amendment when the purpose of the picketing was to compel a company to unlawfully enter into an agreement in restraint of trade). Petrovic threat-

---

[2] "Whoever ... with the intent ... to ... injure, harass, or place under surveillance with intent to ... injure, harass, or intimidate, or cause substantial emotional distress to a person in another State ... uses the mail, any interactive computer service, or any facility of interstate or foreign commerce to engage in a course of conduct that causes substantial emotional distress to that person or places that person in reasonable fear of ... serious bodily injury ... shall be punished as provided in section 2261(b) of this title."

ened to destroy M.B.'s reputation if she terminated their sexual relationship. When M.B. ended the relationship, Petrovic carried out this threat. Petrovic also threatened to continue the humiliating communications unless M.B. paid him $100,000, and when M.B. did not comply, Petrovic carried out this threat for continuing harassment as well. Because Petrovic's harassing and distressing communications were integral to his criminal conduct of extortion under § 875(d), the communications were not protected by the First Amendment.

Furthermore, "where matters of purely private significance are at issue, First Amendment protections are often less rigorous ... because restricting speech on purely private matters does not implicate the same constitutional concerns as limiting speech on matters of public interest." *Snyder v. Phelps*, 562 U.S. ___ (2011). We previously have held that in "extreme case[s]" it is "constitutionally permissible for a governmental entity to regulate the public disclosure of facts about private individuals." *Coplin v. Fairfield Pub. Access Television Comm.*, 111 F.3d 1395, 1404 (8th Cir. 1997). "[A]bsent a compelling state interest," such speech

> can be regulated ... because of its constitutionally proscribable content only if: (1) any such regulation is viewpoint-neutral; (2) the facts revealed are not already in the public domain; (3) the facts revealed about the otherwise private individual are not a legitimate subject of public interest; and (4) the facts revealed are highly offensive.

Id. at 1405.

M.B. was a private individual, and Petrovic's communications revealed intensely private information about M.B. *See id.* at 1404-05. Applying the *Coplin* test, the interstate stalking statute is viewpoint neutral. It proscribes stalking and harassing conduct without making the further content discrimination of proscribing only certain forms of that conduct. *See R.A.V. v. City of St. Paul, Minn.,* 505 U.S. 377, 384 (1992). Second, the intimately private facts and photographs revealed by Petrovic were never in the public domain before Petrovic began his campaign to humiliate M.B. Third, the public has no legitimate interest in the private sexual activities of M.B. or in the embarrassing facts revealed about her life. Finally, the information Petrovic publicized to the community was highly offensive. The communications for which Petrovic was convicted under § 2261A(2)(A) may be proscribed consistent with the First Amendment. The statute is not unconstitutional as applied to Petrovic.

Questions

1. How would *Petrovic* have come out if Petrovic had merely intended to harass M.B., rather than extort her?

2. Compare the *Coplin* test to the elements of the tort of public disclosure of private facts. Are privacy laws automatically constitutional, or do they raise serious First Amendment issues?

3. Petrovic is a man; he wrote insulting and demeaning messages about a woman. Is this a coincidence, or is it part of a larger pattern? Would society be better or worse off with less First Amendment protection for people like him?

True Threats Problems

As noted in *Petrovic*, "true threats," i.e. "unequivocal, unconditional and specific expressions of intention immediately to inflict injury," *United States v. Kelner*, 534 F.2d 1020, 1027 (1976), are unprotected speech. Should it matter whether the speaker subjec-

tively intends to carry out the threat, or only how a reasonable listener would understand it? Are the following true threats?

- A private email by a student to an unknown Internet pen pal, describing the student's fantasy of abducting, raping, and murdering another student in his dorm:

  > 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?

- A Facebook post complaining about the Drug Enforcement Agency:

  > I'll kill whoever I deem to be in the way of harmony to the human reace ... Policeman all deserve to be tortured to death and videos made n sent to their families ... BE WARNED IF U PULL LE OVER!! IM LIKE JASON VOORHEES WITH A BLOODLUST FOR PIG BLOOD.

- A tweet responding to the closure of an airport due to bad weather:

  > Crap! Robin Hood airport is closed. You've got a week and a bit to get your shit together otherwise I'm blowing the airport sky high!!

- An anti-abortion website that features the names of doctors who perform abortions, along with their home addresses and photographs. Beneath each picture, in an Old West-style font, is the logo "WANTED." A legend at the top of the page explains, "Black font (working); Greyed-out Name (wounded); Strikethrough (fatality)."

C. Pornography

This section considers the problem that defined the first generation of mass Internet activism. There were computer *causes célèbres* 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 censor the Internet. The materials walk through the following decade and a half in Internet history.

The section begins start with a quick primer on the Supreme Court's pornography jurisprudence; you should refer back to it regularly. Next, there's a negotiation exercise to help you understand the political climate that produced the Communications Decency Act of 1996 (CDA). The Supreme Court struck down the CDA in *Reno v. ACLU* in 1997, but that didn't stop Congress from trying alternatives. This section concludes 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.

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 any offsetting benefits.

(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." *Miller v. California*, 413 U.S. 15 (1973).

Obscene material can constitutionally be regulated because it has no redeeming social value and its offensiveness provides a positive justification for banning it. 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 – 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, and fine television stations over Janet Jackson's nationally televised, breast-baring "wardrobe malfunction." See *Federal Communications Commission v. Pacifica Foundation*, 438 U.S. 726 (1978); Complaints Against Various Television Licensees Concerning Their February 1, 2004 Broadcast, 21 FCC Rcd. 2760 (2006). In both cases, though it is lawful for adults to receive and exchange such material, children might be watching, and 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. It can 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." It's not usually a meaningful category for First Amendment purposes. Instead, arguments typically need to work within one of the above three categories – that the pornography has no redeeming value, that it depicts children, or that it is being shown to minors.

Question

Which community's "contemporary community standards" define whether material appeals to the prurient interest under the *Miller* test? Pre-Internet law was clear:

> There is no constitutional barrier under Miller to prohibiting communications that are obscene in some communities under local standards even though they are not obscene in others. If Sable's audience is comprised of different communities with different local standards, Sable ultimately bears the burden of complying with the prohibition on obscene messages.

Ashcroft v. American Civil Liberties Union, 535 U.S. 564, 581 (quoting *Sable Communications of Cal., Inc., v. FCC*, 492 U.S. 115, 125–26 (1989). Is this rule as viable for email as it is for postal mail? If local community standards are problematic, what should replace them? National community standards? And if local community standards are problematic, does that also call into question the rule that measuring a work against community standards is a question for the jury?

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 and published in the *Georgetown Law Journal* surveyed almost a million images, descriptions, stories, and animations. It 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.

On 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.

- **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 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 much like pornography, but they will defend anyone's rights to free speech online. These groups 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 frustrated 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. Some of these Internet-focused companies are

relatively new at the lobbying table, but the telecommunications industry in general has been throwing a lot of money around as Congress prepares to pass a major overhaul of telecommunications laws.

• **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 a 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 is also on the table.

Reno v. American Civil Liberties Union

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 Telecommunications Act of 1996 was an unusually important legislative enactment. ... An amendment offered in the Senate was the source of the two statutory provisions challenged in this case. They are informally described as the "indecent transmission" provision and the "patently offensive display" provision ... 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). ...

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 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. 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). ...

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. 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. 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. …

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." 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," 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. ...

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 this from happening? How easy would it be for a child molester to find the ten-year-old?

2. How is it that a statute targeted at protecting *minors* could end up restricting the speech *adults* could receive?

3. If you wanted to post something online and be confident that only adults would see it, what would you do? How confident could you be that no minors were seeing it? How many adults would be wrongfully screened out? Is age-based targeting easier or harder than geographic targeting?

4. In a famous concurrence in part, Justice O'Connor described the CDA as an attempt to create a "zoning law" for the Internet, dividing it into child-safe and adults-only zones. Is it harder or easier to zone the Internet than to zone places? (Both?)

Ashcroft v. Free Speech Coalition

535 U.S. 234 (2002)

Justice Kennedy delivered the opinion of the Court.

We consider in this case whether the Child Pornography Prevention Act of 1996 (CPPA), 18 U.S.C. § 2251 *et seq.*, abridges the freedom of speech. The CPPA extends the federal prohibition against child pornography to sexually explicit images that appear to depict minors but were produced without using any real children. The statute prohibits, in specific circumstances, possessing or distributing these images, which may be created by using adults who look like minors or by using computer imaging. The new technology, according to Congress, makes it possible to create realistic images of children who do not exist. ...

By prohibiting child pornography that does not depict an actual child, the statute goes beyond *New York v. Ferber*, 458 U.S. 747 (1982), which distinguished child pornography from other sexually explicit speech because of the State's interest in protecting the children exploited by the production process. *See id.* at 758. As a general rule, pornography can be banned only if obscene, but under *Ferber*, pornography showing minors can be proscribed whether or not the images are obscene under the definition set forth in *Miller v. California,* 413 U.S. 15 (1973). *Ferber* recognized that "[t]he *Miller* standard, like all general definitions of what may be banned as obscene, does not reflect the State's particular and more compelling interest in prosecuting those who promote the sexual exploitation of children." 458 U.S. at 761.

While we have not had occasion to consider the question, we may assume that the apparent age of persons engaged in sexual conduct is relevant to whether a depiction offends community standards. Pictures of young children engaged in certain acts might be obscene where similar depictions of adults, or perhaps even older adolescents, would not. The CPPA, however, is not directed at speech that is obscene; Congress has proscribed those materials through a separate statute. 18 U.S.C. §§ 1460–1466. Like the law in *Ferber*, the CPPA seeks to reach beyond obscenity, and it makes no attempt to conform to the *Miller* standard. For instance, the statute would reach visual depictions, such as movies, even if they have redeeming social value.

The principal question to be resolved, then, is whether the CPPA is constitutional where it proscribes a significant universe of speech that is neither obscene under *Miller* nor child pornography under *Ferber*.

I

Before 1996, Congress defined child pornography as the type of depictions at issue in *Ferber*, images made using actual minors. 18 U.S.C. § 2252 (1994 ed.). The CPPA retains that prohibition at 18 U.S.C. § 2256(8)(A) and adds three other prohibited categories of speech, of which the first, § 2256(8)(B), and the third, § 2256(8)(D), are at issue in this case. Section 2256(8)(B) prohibits "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." The prohibition on "any visual depiction" does not depend at all on how the image is produced. The section captures a range of depictions, sometimes called "virtual child pornography," which include computer-generated images, as well as images produced by more traditional means. For instance, the literal terms of the statute embrace a Renaissance painting depicting a scene from classical mythology, a "picture" that "appears to be, of a minor engaging in sexually explicit conduct." The statute also prohibits Hollywood movies, filmed without any child actors, if a jury believes an actor "appears to be" a minor engaging in "actual or simulated . . . sexual intercourse." § 2256(2). ...

II ...

The CPPA prohibits speech despite its serious literary, artistic, political, or scientific value. The statute proscribes the visual depiction of an idea – that of teenagers engaging in sexual activity – that is a fact of modern society and has been a theme in art and literature throughout the ages. Under the CPPA, images are prohibited so long as the persons appear to be under 18 years of age. ...

The Government seeks to address this deficiency by arguing that speech prohibited by the CPPA is virtually indistinguishable from child pornography, which may be banned without regard to whether it depicts works of value. *See New York v. Ferber*, 458 U.S., at 761. Where the images are themselves the product of child sexual abuse, *Ferber* recognized that the State had an interest in stamping it out without regard to any judgment about its content. ... The production of the work, not its content, was the target of the statute. The fact that a work contained serious literary, artistic, or other value did not excuse the harm it caused to its child participants. It was simply "unrealistic to equate a community's toleration for sexually oriented materials with the permissible scope of legislation aimed at protecting children from sexual exploitation." *Id.* at 761, n. 12.

Ferber upheld a prohibition on the distribution and sale of child pornography, as well as its production, because these acts were "intrinsically related" to the sexual abuse of children in two ways. *Id.*, at 759. First, as a permanent record of a child's abuse, the continued circulation itself would harm the child who had participated. Like a defamatory statement, each new publication of the speech would cause new injury to the child's reputation and emotional well-being. *See id.*, at 759, and n. 10. Second, because the traffic in child pornography was an economic motive for its production, the State had an interest in closing the distribution network. "The most expeditious if not the only practical method of law enforcement may be to dry up the market for this material by imposing severe criminal penalties on persons selling, advertising, or otherwise promoting the product." *Id.*, at 760. Under either rationale, the speech had what the Court in effect held was a proximate link to the crime from which it came. ...

In contrast to the speech in *Ferber*, speech that itself is the record of sexual abuse, the CPPA prohibits speech that records no crime and creates no victims by its production. Virtual child pornography is not "intrinsically related" to the sexual abuse of children, as were the materials in *Ferber.* 458 U.S., at 759. While the Government asserts that the images can lead to actual instances of child abuse, the causal link is contingent and indirect. The harm does not necessarily follow from the speech, but depends upon some unquantified potential for subsequent criminal acts. ...

III ...

The Government submits further that virtual child pornography whets the appetites of pedophiles and encourages them to engage in illegal conduct. This rationale cannot sustain the provision in question. The mere tendency of speech to encourage unlawful acts is not a sufficient reason for banning it. The government "cannot constitutionally premise legislation on the desirability of controlling a person's private thoughts." *Stanley v. Georgia,* 394 U.S. 557 (1969). First Amendment freedoms are most in danger when the government seeks to control thought or to justify its laws for that impermissible end. The right to think is the beginning of freedom, and speech must be protected from the government because speech is the beginning of thought. ...

The Government next argues that its objective of eliminating the market for pornography produced using real children necessitates a prohibition on virtual images as well. Virtual images, the Government contends, are indistinguishable from real ones; they are part of the same market and are often exchanged. In this way, it is said, virtual images promote the trafficking in works produced through the exploitation of real children. The hypothesis is somewhat implausible. If virtual images were identical to illegal child pornography, the illegal images would be driven from the market by the indistinguishable substitutes. Few pornographers would risk prosecution by abusing real children if fictional, computerized images would suffice. ...

Finally, the Government says that the possibility of producing images by using computer imaging makes it very difficult for it to prosecute those who produce pornography by using real children. Experts, we are told, may have difficulty in saying whether the pictures were made by using real children or by using computer imaging. The necessary solution, the argument runs, is to prohibit both kinds of images. The argument, in essence, is that protected speech may be banned as a means to ban unprotected speech. This analysis turns the First Amendment upside down. ...

Questions

1. How would *Free Speech Coalition* apply to images of adults whose facial features have been altered to make them look like children? Images of actual children's' faces Photoshopped onto images of adults' bodies?

2. Does the Internet make child pornography more or less prevalent? Does it make prosecuting child pornographers easier or harder?

3. Is *Free Speech Coalition* a case about new rules for a new digital era, a case applying old principles to new technologies, or a case in which the computer angle is incidental?

4. Congress responded to *Free Speech Coalition* by enacting a new "pandering and solicitation" statute, which prohibits advertising or distributing "any material or purported material in a manner that reflects the belief, or that is intended to cause another to believe, that the material or purported material is, or contains" child pornography. 18 U.S.C. § 2252A(a)(3)(B). Does the shift from possession to pandering cure the constitu-

tional problem? Is there a legitimate free speech interest in advertising (truthfully or falsely) that material is child pornography?

5. If "virtual" child pornography becomes indistinguishable from child pornography featuring actual children, what obstacles might this present to successfully prosecuting those who make, distribute, and possess child pornography? Are there any evidentiary issues involved in proving that the images found in the defendant's possession were not computer-generated and to the defendant's knowledge. How significant do you think these evidentiary barriers have been in actual prosecutions? Does this blurring of boundaries justify prohibiting "virtual" child pornography?

CPOEA Problem

The federal Child Protection and Obscenity Enforcement Act of 1988 (CPOEA) requires those who create materials depicting "actual sexually explicit conduct" to 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 Act of 2003 (PROTECT Act), extends the records requirement to include digital and computer-manipulated images and videos. It also 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. What result, and why?

D. Filtering

As we have seen on multiple occasions, law is not the only force at work online. Because the Internet is made up of computers, those computers can potentially have their programming changed. If the code changes, so does the regulatory effect. This gives lawmakers an immensely powerful lever to pull: convince or compel companies that operate networks, websites, and other online applications to use their technical power in ways that make the lawmakers' regulatory goals easier to achieve. Thus, our second major theme – governmental power – is closely bound up with the first – code is law.

This section considers governmental attempts to regulate speech not by punishing speakers but instead by changing the programming of the Internet's technical architecture. Filtering has been popular around the world: studies suggest that a majority of countries require some form of Internet filtering. But the details vary widely. China's comprehensive system of filtering, which restricts access to politically sensitive materials on numerous topics, is the best-known. The section continues the chapter's emphasis on the United States legal free speech framework. As the cases illustrate, applying the First Amendment to these Internet filtering involves both conceptual and pragmatic difficulties. As the cases also illustrate, protecting children is far and away the most commonly proffered justification for filtering.

Center for Democracy and Technology v. Pappert

337 F. Supp. 2d 606 (E.D. Pa. 2004)

DuBois, District Judge:

I. Introduction

In February of 2002, Pennsylvania enacted the Internet Child Pornography Act, 18 Pa. Cons. Stat. §§ 7621-7630, ("the Act"). The Act requires an Internet Service Provider ("ISP") to remove or disable access to child pornography items "residing on or accessible through its service" after notification by the Pennsylvania Attorney General. It is the first attempt by a state to impose criminal liability on an ISP which merely provides access to child pornography through its network and has no direct relationship with the source of the content.

The plaintiffs are Center for Democracy and Technology ("CDT"), the American Civil Liberties Union of Pennsylvania ("ACLU"), and Plantagenet, Inc. CDT is a non-profit corporation incorporated for the purpose of educating the general public concerning public policy issues related to the Internet. The ACLU is a non-partisan organization of more than 13,000 members dedicated to defending the principles of liberty and equality embodied in the Bill of Rights. Plantagenet, Inc., is an ISP that provides a variety of services related to the Internet. Defendant is Gerald J. Pappert, Attorney General of the Commonwealth of Pennsylvania. ...

III. Findings of Fact ...

C. Internet Child Pornography Act ("The Act") ...

The Act permits defendant or a district attorney in Pennsylvania to seek a court order requiring an ISP to "remove or disable items residing on or accessible through" an ISP's service upon a showing of probable cause that the item constitutes child pornography. The application for a court order must contain the Uniform Resource Locator providing access to the item.

Child pornography is defined as images that display a child under the age of 18 engaged in a "prohibited sexual act." A prohibited sexual act is defined as "sexual intercourse . . . masturbation, sadism, masochism, bestiality, fellatio, cunnilingus, lewd exhibition of the genitals or nudity if such nudity is depicted for the purpose of sexual stimulation or gratification of any person who might view such depiction."

The court order may be obtained on an *ex parte* basis with no prior notice to the ISP or the web site owner and no post-hearing notice to the web site owner.

Under the Act, a judge may issue an order directing that the challenged content be removed or disabled from the ISP's service upon a showing that the items constitute probable cause evidence of child pornography. A judge does not make a final determination that the challenged content is child pornography.

Once a court order is issued, the Pennsylvania Attorney General notifies the ISP in question and provides the ISP with a copy of the court order. The ISP then has five days to block access to the specified content or face criminal liability, including fines of up to $30,000 and a prison term of up to seven years.

According to defendant, the purpose of the Act is: "To protect children from sexual exploitation and abuse. To serve this purpose by interfering with distribution of child pornography, particularly its distribution over the Internet."

Government law enforcement agencies have attempted to locate and criminally prosecute persons who produce or knowingly distribute child pornography. However, a state agency in the United States cannot easily prosecute producers and distributors of child pornography because they are rarely found in that particular state and often are not found in the United States. ...

E. ISP Compliance with Court Orders or Informal Notices ...

2. Methods of Implementation

According to the ISPs, on most occasions, they attempted to comply with the Informal Notices by implementing either IP filtering or DNS filtering. These methods were either used alone or together.

Use of IP filtering, DNS filtering, or URL filtering to block content accessible through the service of an ISP only affects Internet users who access the Internet through that ISP's service. Thus, Internet users that do not use the service of an ISP that blocked a web site would still have access to the blocked content.

a. DNS Filtering

To perform DNS filtering, an ISP makes entries in the DNS servers under its control that prevent requests to those servers for a specific web site's fully qualified domain name (found in the requested site's URL) from resolving to the web site's correct IP address. The entries cause the DNS servers to answer the requests for the IP addresses for such domain names with either incorrect addresses or error messages. Without the correct IP addresses of the requested sites, the requests either do not proceed at all or do not reach the desired sites.

b. IP Filtering ...

To implement IP filtering, an ISP first determines the IP address to which a specific URL resolves. It then makes entries in routing equipment that it controls that will stop all outgoing requests for the specific IP address.

c. URL Filtering

Mr. Stern testified that ISPs could comply with blocking orders using URL filtering. ... URL filtering involves the placement of an additional device, or in some cases the reconfiguration of an existing "router" or other device, in the ISP's network to (a) reassemble the packets for Internet traffic flowing through its network, (b) read each http web request, and (c) if the requested URL in the web request matches one of the URLs specified in a blocking order, discard or otherwise block the http request.

3. Comparison of Filtering Methods

a. Ease of Implementation and Cost ...

Most ISPs already have the hardware needed to implement IP filtering and IP filtering is a fairly routine aspect of the management of a network. IP filtering is used to respond to various types of attacks on a network, such as denial of service attacks and spam messages. ... For AOL, IP filtering is "in common use as a defensive mechanism against such activities as virus proliferation, spam, et cetera. It is a basic and common tool of the trade."...

Most ISPs that do not outsource Internet access would not be required to purchase new equipment to implement DNS filtering. If the ISP's staff is familiar with this method of filtering, the necessary entries in the DNS servers require no expenditure of money and little staff time. ...

No ISPs known to either plaintiffs' or defendant's experts utilize URL filtering to screen all World Wide Web traffic. ...

If an ISP did not purchase substantially more switches and routers, URL filtering would "significantly degrade" the performance of an ISP's network. Such degradation is caused by the fact that the technical process of comparing all of the URLs in the web traffic flowing through an ISP's network with a list of URLs to be blocked is "expensive" in the computational sense – it requires a significant amount of computing power. Performing these computations would slow down each switch and router substantially and decrease the overall capacity of the network. ...

The purchase and testing of the equipment necessary to perform URL filtering would require a significant investment by ISPs. ... It would cost Verizon "well into seven figures" to implement URL filtering across its entire network. "[M]oney aside, the current [URL filtering] technology ... would not be able to even operate in [WorldCom's] network" because the current URL filtering products (a) cannot support the speeds needed in WorldCom's network and (b) do not connect to the type of physical wiring (such as fiber optic and coaxial copper cable) that WorldCom uses. ...

c. Overblocking

DNS filtering stops requests for all sub-pages under the blocked domain name. Thus, if the domain name included in the URL identified by an Informal Notice is of a Web Hosting Service that allows users to post their independent content as sub-pages on the service's site, the DNS server entries will stop requests for all of the independent pages on the service, not just the page that displays the targeted child pornography item. For example, DNS filtering results in overblocking when an online community such as the GeoCities web site, which allows many different users to have web sites on sub-pages of GeoCities.com, is targeted by an Informal Notice. ...

IP filtering leads to a significant amount of overblocking. As Mr. Stern stated, IP filtering "will block innocent sites to a great deal," and "IP address filtering is extremely likely to block untargeted sites due to the process known as virtual hosting," ...

IP filtering leads to blocking, of innocent web sites, because of the prevalence of shared IP addresses. … If an ISP uses IP filtering to block access to a particular IP address, all web sites hosted at that IP address are blocked. As an example, in response to Informal Notice 2545, Epix.net blocked access to IP address 204.251.10.203, which in turn blocked access to two of Laura Blain's web sites and others hosted by directNIC.

URL filtering filters out URLs down to the specific subpage. It presents no risk of disabling access to untargeted sites.

Although URL filtering results in the least amount of overblocking, no ISPs are currently capable of implementing this method. Both DNS filtering and IP filtering result in overblocking. …

8. Methods of Evasion

a. Anonymous Proxy Servers

Internet users who want to keep their identity secret can use anonymous proxy servers or anonymizers. In the context of visiting web sites, these services route all requests through the proxy server or anonymizer, which in turn sends the request to the desired web site. Requests using these services appear to the ISP routing the request as if they are requests directed to the proxy service, not to the underlying URL to which the user actually seeks access.

The use of anonymous proxy services or anonymizers completely circumvents both of the technical blocking methods – IP filtering and DNS filtering – used by the ISPs to comply with the Informal Notices and would circumvent URL filtering as well. For example, web sites blocked by AOL could be accessed through AOL's service using the anonymizer "Proxify.com."

If the child pornography seeker chooses to have all of his web requests run through a proxy or anonymizer, he faces obstacles and risks. First, he must learn how to configure his computer to do so. This requires a number of difficult entries. Second, even if he successfully configures his computer, the seeker must then accept the risks of a reconfiguration that sends all requests through another computer that the user does not control – risks that the connection will not work or that the service will be slow. …

b. The Ability of Child Pornographers to Evade Filters …

IP filtering can be evaded by operators of child pornography sites by changing the IP address of the web site. In one instance, the OAG sent a second Informal Notice relating to one site because it had become available to AOL users at a different IP address after AOL blocked the original IP Address. AOL responded by blocking the second IP address as well.

Operators of child pornography sites can use a range of methods to evade DNS filtering, including: (1) using an IP address as a URL, i.e., a web site can use an IP address (or string of numbers) as the URL instead of a domain name like "www.example.com"; or (2) changing a portion of a domain name and promulgating the new domain name in hyperlinks to the web site in advertisements, search engines or newsgroups. …

IV Conclusions of Law …

B. Substantive First Amendment Issuses …

1. Burden on Speech

Defendant proposes that the "only reasonable means" test should be used to determine whether the Act burdens speech. Under defendant's test, the Act is constitutional unless the only reasonable means of compliance requires blocking protected speech.

Plaintiffs argue that if the effect of the Act has been to block protected speech, the Act is subject to First Amendment scrutiny.

This case is unusual in that the Act, on its face, does not burden protected speech. Facially, the Act only suppresses child pornography, which can be completely banned from the Internet. However, the action taken by private actors to comply with the Act has blocked a significant amount of speech protected by the First Amendment. *United States v. Playboy Entertainment Group*, 529 U.S. 803 (2000), relied upon by both parties, is the case that comes closest to addressing how this type of burden on protected speech should be addressed.

The federal statute at issue in *Playboy* required cable operators which provided sexually oriented programing to either fully scramble or block the channels that provided this programming, or limit the transmission of such programming to the hours between 10:00 P.M., and 6:00 A.M., referred to as "time channeling." The Supreme Court determined that the statute was unconstitutional because the government failed to establish that the two methods for compliance identified in the challenged section were the least restrictive means for achieving the government's goal. ...

The analysis of the *Playboy* Court is particularly instructive in this case. That is so because the majority of cable operators involved in that case chose to comply with the section of the statute at issue by using time channeling notwithstanding the fact that it silenced a significant amount of protected speech, whereas the other stated method of compliance, scrambling, did not. On that issue, the Court ruled that a reasonable cable operator could choose not to use the scrambling alternative provided by the statute because the available scrambling technology was "imprecise" and portions of the scrambled programs could be heard or seen by viewers, a phenomenon known as "signal bleed." Thus, "[a] rational cable operator, faced with the possibility of sanctions for intermittent bleeding, could well choose to time channel even if the bleeding is too momentary to pose any concern to most households." *Id.* at 821. The Court also noted that digital technology would have solved the signal bleed problem, but it was "not in wide-spread use."

The basis for the *Playboy* Court's determination that the statute was not the least restrictive means for achieving the government's goal was the fact that time channeling, deemed to be a reasonable method of compliance for cable operators, silenced "protected speech for two-thirds of the day in every home in a cable service area, regardless of the presence or likely presence of children or of the wishes of viewers." *Id.* In making this statement, the Court determined that "targeted blocking" at the request of a customer was a "less restrictive" and feasible means of furthering the government's compelling interest in the case. *Id.* at 816, 827. Targeted blocking required cable operators to block sexually-oriented channels at individual households. It was deemed to be less restrictive in that it enabled parents who did not want their child exposed to the program to block the offending channels without depriving willing viewers of the opportunity to watch a particular program.

The Act in this case has resulted in the blocking of in excess of 1,190,000 web sites that were not targeted by the Informal Notices. Defendant argues that this overblocking does not violate the First Amendment because it resulted from decisions made by ISPs, not state actors. According to defendant, ISPs have "options for disabling access that would and will not block any, or as many, sites as Plaintiffs claim were blocked in the past" and the choice of which filtering method to use was "completely the decision of the ISPs."

The Court rejects this argument. Like the statute analyzed in *Playboy*, the Act in this case provides ISPs with discretion to choose a method of compliance although such

methods are not incorporated in the Act itself. Like the time channeling in *Playboy*,the court concludes that ISPs could reasonably choose IP filtering and DNS filtering in order to comply with Act. And, like Playboy, the alternatives reasonably available to the ISPs block protected speech to a significant degree.

The two filtering methods used by the ISPs to comply with the Informal Notices and the court order — IP filtering and DNS filtering — both resulted in overblocking. IP filtering blocks all web sites at an IP address and, given the prevalence of shared IP addresses, the implementation of this method results in blocking of a significant number of sites not related to the alleged child pornography. As an example, access to Ms. Blain's web sites and over 15,000 other sites was blocked to Epix users as a result of the IP Filtering Epix implemented to comply with Informal Notice 2545. Filtering also results in overblocking when the method is used to block a web site on an online community or a Web Hosting Service, or a web host that hosts web sites as sub-pages under a single domain name. Specifically, Verizon blocked hundreds of thousands of web sites unrelated to the targeted child pornography when it used DNS filtering to block access to a sub-page of the Terra.es web site, a large online community, in response to Informal Notice 5924. One of the web sites blocked was for a Spanish geological survey, and defendant acknowledged that this web site did not contain child pornography. Although a small subset of web hosts, Web Hosting Services host a large number of web sites and the OAG admitted that they are not always identifiable based on the URL. In fact, the OAG continued to issue notices to Web Hosting Services after it was aware of the overblocking problem and had implemented a new procedure to deal with these services.

Moreover, contacting the web host is not a legitimate alternative to use of technical filtering methods. ISPs will not always be able to contact the host within the time period provided by the Act. Even if they can contact a host, the host may not be willing to remove the offending content. In either event, the ISP would be forced to use IP filtering or DNS filtering to disable access. In addition, an ISP using this method of compliance risks criminal prosecution if the host decides to place the offending content back on the Internet. Thus, it is rational for an ISP to implement a method of compliance that is not based on the actions of a third party.

The Court will evaluate the constitutionality of the Act with respect to the technology that is currently available. The *Playboy* Court did not consider digital technology a feasible alternative because it was not "economical" for cable operators to use this technology. Similarly, in *Reno v. ACLU*, 521 U.S. 844 (1997), the Supreme Court rejected an argument that Internet content providers could rely on "tagging" or credit card verification technology because the proposed screening software did not exist at that time. ...

The URL filtering technology recommended by the OAG at trial was not available to any ISPs that received Informal Notices or a court order, with the exception of AOL. AOL's use of URL filtering was limited; it could not use URL filtering on its entire network. The evidence establishes that it would not be economical for ISPs to develop and implement URL filtering technology. Even if the ISPs invested in the development of this technology, it would take a significant amount of research and testing to implement this filtering method and none of the experts or engineers who testified were able to give a timetable for the completion of this research. Moreover, if the ISPs were able to develop the devices and software necessary to perform URL filtering, they would be required to purchase "substantially more" switches and routers to avoid "significantly" degrading the performance of their networks. Given the uncertain nature of the research, it is difficult to predict the cost of developing this technology. However, one expert estimated that it would cost the ISP that employs him, Verizon, "well into seven figures" to implement URL

filtering across its entire network. Thus, URL filtering is not a feasible alternative to DNS filtering and IP filtering.

As this Court reads *Playboy*, if a statute regulating speech provides distributors of speech with alternatives for compliance and the majority of distributors reasonably choose an alternative that has the effect of burdening protected speech, the statute is subject to scrutiny as a burden on speech. Both of the filtering methods used by the ISPs in response to Informal Notices and the court order issued in this case resulted in the blocking of innocent speech. The method of filtering recommended by defendant at trial — URL filtering — was rejected by the ISPs as infeasible. As a result, the Court concludes that the Act burdens speech and is subject to First Amendment scrutiny.

2. Level of Scrutiny

[The court considered two possible standards of review. The plaintiffs argued for strict scrutiny, because the Act was a content-based restriction on speech. The defendants argued for intermediate scrutiny because the Act was targeted at unprotected speech but had incidental effects on protected speech.]

Although there are strong arguments for the application of strict and intermediate scrutiny, the Court need not choose between the two because, even under the less demanding standard — intermediate scrutiny — the Act does not pass Constitutional muster. Under *O'Brien*, a regulation must further an important government interest unrelated to the suppression of free expression and the incidental restriction on First Amendment freedoms must be no greater than is essential to the furtherance of that interest. The government has the burden of proving that the "regulation will in fact alleviate [the] harms [addressed by the regulation] in a direct and material way," *Turner* [*Broad. Sys. v. FCC*], 512 U.S. at 664, and it has not met that burden in this case. In addition, the Act suppresses substantially more protected material than is essential to the furtherance of the government's interest in reducing child sexual abuse.

Although the prevention of child exploitation and abuse is an state interest unrelated to the suppression of free expression, defendant has not produced any evidence that the implementation of the Act has reduced child exploitation or abuse. The Act does block some users' access to child pornography; however, the material is still available to Internet users accessing the material through ISPs other than the one that blocked the web site. In addition, there are a number of methods that users and producers of child pornography can implement to avoid the filtering methods. For example, both IP filtering and DNS filtering can be avoided by a person using an anonymous proxy server or an anonymizer. A child pornographer can evade an IP filter by moving his web site to another IP address without having to change the content or the URL identifying the site. A user attempting to evade a DNS filter can manually enter the IP address for a DNS server not controlled by his ISP to avoid the block. Moreover, there is no evidence that any child pornographers have been prosecuted as a result of defendant's enforcement of the Act. In fact, the OAG did not investigate the entities that produce, publish, and distribute the child pornography. Although the inference could be drawn that making it more difficult to access child pornography reduces the incentive to produce and distribute child pornography, this burden on the child pornography business is not sufficient to overcome the significant suppression of expression that resulted from the implementation of the Act.

More than 1,190,000 innocent web sites were blocked in an effort to block less than 400 child pornography web sites, and there is no evidence that the government made an effort to avoid this impact on protected expression. As discussed in the previous section of this Memorandum, all the currently available technical methods of disabling

access to a web site accessible through an ISP's service result in significant overblocking. The Act fails to specify any means of compliance, let alone provide guidance as to which method will minimize or avoid suppression of protected speech. This burden on protected expression is substantial whereas there is no evidence that the Act has impacted child sexual abuse. Thus, the Act cannot survive intermediate scrutiny. ...

C. Procedural First Amendment Issues

1. Prior Restraint

The Act and Informal Notice process are not prior restraints in the traditional sense. They do not prevent speech from reaching the market place but remove material already available on the Internet from circulation. *Alexander v. United States*, 509 U.S. 544 (1993) ("The term 'prior restraint' describes orders forbidding certain communications that are issued before the communications occur.") However, they are administrative prior restraints as that term has been interpreted by the Supreme Court. According to the Court, "only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression, only a procedure requiring a judicial determination suffices to impose a valid final restraint." *Freedman v. Maryland*, 380 U.S. 51, 58 (1965). Thus, if material protected by the First Amendment is removed from circulation without these procedural protections, the seizure is invalid as a prior restraint. The Court used the term to describe a Rhode Island Commission's practice of sending letters to book distributors that asked the distributors to remove books from circulation in *Bantam Books v. Sullivan*, 372 U.S. 58 (1963) and a procedure that allowed courts to order pre-trial seizure of films alleged to be obscene in *Fort Wayne Books, Inc. v. Indiana*, 489 U.S. 46, 51-52, 109 S.Ct. 916, 103 L.Ed.2d 34 (1989). ...

Based on the decision in *Bantam Books* and *Fort Wayne Books*, this Court concludes the procedural protections provided by the Act are inadequate. These cases require a court to make a final determination that material is child pornography after an adversary hearing before the material is completely removed from circulation. Under the Act, a judge is only required to make a finding of probable cause, he can make this determination *ex parte*, and there is no requirement that the publisher or distributor receive notice or an opportunity to be heard.

Additionally, as argued by plaintiffs, the Act allows for an unconstitutional prior restraint because it prevents future content from being displayed at a URL based on the fact that the URL contained illegal content in the past. Plaintiffs compare this burden to the permanent ban on the publication of a newspaper with a certain title, *Near v. Minnesota*, 283 U.S. 697 (1931), or a permanent injunction against showing films at a movie theater, *Vance v. Universal Amusement Co.*, 445 U.S. 308 (1980). In *Near*, the Court examined a statute that provided for a permanent injunction against a "malicious, scandalous, and defamatory newspaper, magazine or other periodical." *Near*, 283 U.S. at 701-702, *Near* involved a county attorney who obtained an injunction against the publishers of a newspaper called "The Saturday Press" under a statute preventing them from "publishing, circulating, or having in their possession any future editions of said The Saturday Press." *Id.* at 705. The statute at issue in Near was held to be unconstitutional because it permitted censorship of future publications based on material published in the past.

There are some similarities between a newspaper and a web site. Just as the content of a newspaper changes without changing the title of the publication, the content identified by a URL can change without the URL itself changing. In fact, it is possible that the owner or publisher of material on a web site identified by a URL can change without the URL changing. Plaintiffs demonstrated this by purchasing the

http://www.littleangels.tv/tr URL and converting the alleged child pornography web site into a web site dedicated to a description of this case. ... Despite the fact that the content at a URL can change frequently, the Act does not provide for any review of the material at a URL and, other than a verification that the site was still blocked thirty days after the initial Informal Notice, the OAG did not review the content at any blocked URLs. Moreover, other than the instances in which complaints were made about blocked innocent content, ISPs have continued to maintain their blocking action. Specifically, WorldCom, Comcast, AOL, and Verizon all testified that they routinely maintain the blocks implemented in response to Informal Notices or, with respect to World Com, the court order. ...

The fact that an ISP can challenge a judge's child pornography determination in a criminal prosecution does not save the Act. Only one ISP, WorldCom, challenged an Informal Notice and then promptly complied with a court order obtained by the OAG. An ISP has little incentive to challenge the suppression of a web site with which it has no business relationship. As stated by the Supreme Court, a statute that suppresses speech "must be tested by its operation and effect." *Near v. Minnesota*, 283 U.S. 697, 708 (1931). The operation and effect of this Act is that speech will be suppressed when a court order is issued, and the procedural protections provided by the Act before the order can issue are insufficient to avoid constitutional infirmity. ...

Questions

1. How is the filtering problem faced by ISPs dealing with Pennsylvania like the filtering problem faced by Yahoo! dealing with France? How is it different?

2. Why is filtering hard? Would it be possible to create a filter that never let a child pornography website through? One that never blocked an innocent site? Would you want to subscribe to an ISP that used one of these filters?

3. Will ISPs subject to the Act err on the site of blocking too many websites, or too few?

4. Would the result in *Pappert* have been different if Pennsylvania had ordered ISPs to filter out some other category of websites, such as websites criticizing the governor, or websites offering illegal prostitution services?

5. It has become cheaper and easier for ISPs to detect, in real time, which URLs their subscribers are visiting. Indeed, some ISPs have used this technology to identify subscribers' interests to show them targeted ads. Would the Act be constitutional if all ISPs could use URL filtering at low cost?

6. Does the Act have any other legal problems? Some of the ISPs were only able to add filters to their entire network, not just the portions serving Pennsylvania. Does the statute violate the Dormant Commerce Clause? Keep the statute in mind as you read the materials on Section 230 in the next section.

7. Would the Act be constitutional if it applied only to public libraries? If it were phrased as a condition of state funding for local libraries rather than as a command? Would it matter whether the filters could be disabled at the request of a patron?

COPA Problem

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 *Miller* definitions, but it tacks 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 nar-

rowly tailored and because filtering software installed on children's computers by their guardians would be a less restrictive alternative. What result, and why?

E. Section 230

Although the anti-indecency portions of the Communications Decency Act were held unconstitutional by the Supreme Court in *Reno*, another provision of the CDA has had a much more successful run. Telecommunications companies, concerned about their potential liability for offensive material posted by users, successfully lobbied Congress for statutory immunity. It was codified at 47 U.S.C. § 230 and is frequently referred to simply as "Section 230." It is, bar none, the single most important piece of law discussed in this book.

The basic idea of Section 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 late 1990s. The courts have chosen to interpret Section 230 broadly – creating a kind of immunity with no offline parallel. The first case in this section – *Zeran* – illustrates the crucial early decisions by the courts to read Section 230's immunities broadly. Although the subsequent cases will point out some of the factors that have made *Zeran* controversial, that controversy is not reflected in the trend of judicial decisions, which overwhelmingly agree with its holding.

The cases in this section heavily explore the book'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 read these materials, ask yourself what goals that immunity is meant to serve, and who else benefits (or loses) when intermediaries are empowered in this way. These cases also raise the book's fourth major theme: innovation on the Internet. Some scholars have argued that Section 230 has played a substantial role in encouraging the development of the Internet as a commercial and social resource. As you read, ask yourself how an intermediary immunity could be considered a kind of subsidy for entrepreneurialism online.

Restatement (Second) of Torts

§ 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.

Questions

1. The Internet is famously capable of behaving like all sorts of different media: you can get movies, television, radio, newspapers, magazines, party invitations, and personal letters online. In media circles, this phenomenon is known as *convergence*. Does Twitter seem more like a letter, a telephone conversation, a newspaper, a public speech, or a television broadcast? What about email? The Web?

2. Clark Kent writes a false and injurious article accusing businessman Lex Luthor of involvement in criminal activity. The *Daily Planet* newspaper prints the article on its front page. Olsen Newsstands sells the papers to the public. Slow Lane Coffee has several copies set out for its patrons. Which of them are liable to Luthor for defamation? What if Luthor notifies them of the article's falsity? What if the article is published on `dailyplanet.com` instead?

47 U.S.C. § 230

§ 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).

...

(e) Effect on other laws

(1) No effect on criminal law

Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute.

(2) No effect on intellectual property law

Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

...

(f) Definitions

As used in this section:

...

(2) Interactive computer service

The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

(3) Information content provider

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. ...

Question

1. *Before* you read further, what do you think Section 230 means? What kinds of entities qualify for the immunity, from what kinds of liability, and under what circumstances? Does it adopt the Restatement's rules, or change them? Now read on.

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*, 521 U.S. 844, 849, (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, so we accept the facts alleged in the complaint as true. 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 Okla-

homa 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.[1] 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

---

[1] Zeran maintains that AOL made it impossible to identify the original party by failing to maintain adequate records of its users. The issue of AOL's record keeping practices, however, is not presented by this appeal.

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, 521 U.S. at 849 (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. 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 (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 self-regulation.

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.

Questions

1. *Zeran* is one of the most important texts in all of Internet law. It rewards careful reading. State the post-*Zeran* rule of Section 230 in your own words, in one sentence.

2. Explain the distinction between "publisher" and "distributor" liability at common law. The`n explain *Zeran's* holding in terms of these categories. Now explain it again, slowly. N`ow 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.

3. Why did Ken Zeran need to sue AOL? Couldn't he have sued the user who posted the fake ads?

4. How would AOL have to change the way it does business if it were treated as a distributor? If it were treated as a publisher? What about YouTube, to which users upload hundreds of thousands of videos daily?

5. Is *Zeran* an extension of offline principles to Internet activity, or does it create a new, Internet-only legal regime?

6.Why do opponents of Section 230 say that its effects are toxic in giving intermediaries no incentives to be responsible Internet citizens? How would proponents of Section 230 respond?

Jones v. Dirty World Entertainment Recordings LLC

--- F.3d --- (6th Cir. June 16, 2014)

Gibbons, Circuit Judge:

This case presents the issue of whether the Communications Decency Act of 1996 (CDA), 47 U.S.C. § 230, bars the state-law defamation claims of plaintiff-appellee Sarah Jones. Jones was the unwelcome subject of several posts anonymously uploaded to www.TheDirty.com, a popular website operated by defendants-appellants Nik Lamas–Richie and DIRTY WORLD, LLC ("Dirty World"), and of remarks Richie posted on the site. The website enables users to anonymously upload comments, photographs, and video, which Richie then selects and publishes along with his own distinct, editorial comments. In short, the website is a user-generated tabloid primarily targeting nonpublic figures.

In response to the posts appearing on www.TheDirty.com, Jones brought an action in federal district court alleging state tort claims of defamation, libel *per se,* false light, and intentional inflection of emotional distress. Richie and Dirty World claimed that § 230(c)(1) barred these claims. The district court rejected this argument and denied defendants-appellants' motion to dismiss, motion for summary judgment, motion to revise judgment, and motion for judgment as a matter of law. The district court also denied Richie's and Dirty World's motion for leave to file an interlocutory appeal. The case was submitted to a jury, twice. The first trial ended in a mistrial upon a joint motion. The second trial resulted in a verdict in favor of Jones for $38,000 in compensatory damages and $300,000 in punitive damages. On appeal, Richie and Dirty World maintain that § 230(c)(1) barred Jones's claims. ...

I.

Richie is currently employed as the manager of DIRTY WORLD, LLC ("Dirty World"), which owns and operates the website www.TheDirty.com. ... The website receives approximately six hundred thousand visits each day and eighteen million visits each month.

As the website grew, its focus and format changed. In the beginning, Richie created nearly all the content on the site, and users could not directly upload content. This is no longer true. For the past several years and currently, users of the site, who colloquially refer to themselves as "The Dirty Army," may submit "dirt"—*i.e.*, content that may include text, photographs, or video about any subject. Users may also post comments about the content submitted by others. The vast majority of the content appearing on www.TheDirty.com is comprised of submissions uploaded directly by third-party users.

The content submission form instructs users to "Tell us what's happening. Remember to tell us who, what, when, where, why." The content submission form requires users to submit a title and category for their submission as well as their city or college for indexing. Submissions appear on the website as though they were authored by a single, anonymous author—"THE DIRTY ARMY." This eponymous introduction is automatically added to every post that Richie receives from a third-party user. Many, but not all, of the submissions and commentaries appearing on the website relate to stories, news, and gossip about local individuals who are not public figures. The site receives thousands of new submissions each day. Richie or his staff selects and edits approximately 150 to 200 submissions for publication each day. The editing done to published submissions only consists of deletion. Richie or his staff briefly reviews each submission selected for publication to ensure that nudity, obscenity, threats of violence, profanity, and racial slurs are removed. Richie typically adds a short, one-line comment about the post with "some sort of humorous or satirical observation." Richie, however, does not materially change, create, or modify any part of the user-generated submission, nor does he fact-check submissions for accuracy. Apart from his clearly denoted comments appended at the end of each submission, which appear in bold-face text and are signed "-nik," Richie does not create any of the posts that appear on www.TheDirty.com. The bold-face text and signature are designed to distinguish editorial remarks from third-party submissions. Comments that appear in bold face and are signed "-nik" are only written and published by Richie.

Sarah Jones is a resident of northern Kentucky. Jones was a teacher at Dixie Heights High School in Edgewood, Kentucky, and a member of the Cincinnati BenGals, the cheerleading squad for the Cincinnati Bengals professional football team. From October 2009 to January 2010, Jones was the subject of several submissions posted by anonymous users on www.TheDirty.com and of editorial remarks posted by Richie.

First, on October 27, 2009, a visitor to www.TheDirty.com submitted two photographs of Jones and a male companion and the following post:

> THE DIRTY ARMY: Nik, this is Sara J, Cincinnati Bengal Cheerleader. She's been spotted around town lately with the infamous Shayne Graham. She has also slept with every other Bengal Football player. This girl is a teacher too!! You would think with Graham's paycheck he could attract something a little easier on the eyes Nik!

Appearing directly beneath this post, Richie added:

> Everyone in Cincinnati knows this kicker is a Sex Addict. It is no secret ... he can't even keep relationships because his Red Rocket has freckles that need to be touched constantly.—nik

Jones requested that the post be removed. Richie informed Jones that the post would not be removed.

Second, on December 7, 2009, a visitor submitted a photograph of Jones and the following post:

> THE DIRTY ARMY: Nik, here we have Sarah J, captain cheerleader of the playoff bound cinci bengals.. Most ppl see Sarah has [sic] a gorgeous cheerleader AND highschool teacher.. yes she's also a teacher.. but what most of you don't know is.. Her ex Nate.. cheated on her with over 50 girls in 4 yrs.. in that time he tested positive for Chlamydia Infection and Gonorrhea.. so im sure Sarah also has both.. whats worse is he brags about doing sarah in the gym .. football field.. her class room at the school she teaches at DIXIE Heights.

Appearing directly after this post, Richie remarked: "Why are all high school teachers freaks in the sack?nik"

Third, on December 9, 2009, a visitor submitted another photograph of Jones and a male companion and the following post:

> THE DIRTY ARMY: Nik, ok you all seen the past posting of the dirty Bengals cheerleader/teacher ... well here is her main man Nate. Posted a few pics of the infected couple. Oh an for everyone saying sarah is so gorgeous check her out in these non photoshopped pics.

Appearing directly after this post, Richie added:

> Cool tribal tat man. For a second yesterday I was jealous of those high school kids for having a cheerleader teacher, but not anymore.—nik

Jones sent Richie over twenty-seven emails, pleading for Richie to remove these posts from the website, to no avail. Jones's father similarly wrote to Richie, also to no avail. She then sought legal help, and her attorney informed Richie that if the posts were not removed by December 14, 2009, Jones would file suit. The posts were not removed. Jones, *qua* Jane Doe, filed in federal district court this action on December 23, 2009, against Dirty World Entertainment Recordings, LLC, which operated a website called www.thedirt.com. Apparently, Jones sued the wrong party, as neither Richie nor Dirty World has or ever had any relationship with either Dirty World Entertainment Recordings, LLC, or www.thedirt.com. Nevertheless, the lawsuit sparked national media attention, which precipitated further postings on www.TheDirty.com regarding Jones.

For instance, on December 29, a visitor submitted a photograph and the following post:

> THE DIRTY ARMY: Nik, i just saw the Huffington Post and I just [sic] the latest post on beat Bang–GALS cheer squad and back in May I was out clubbing in Cinci and those cheer chicks were hosting the club and i could not believe how ugly they were, here is some pics of them from that night.

Richie added:

> I think they all need to be kicked off and the Cincinnati Bengals should start over. Note to self: Never try to battle the DIRTY ARMY.—nik ...

... After the litigation commenced, Richie posted a public letter to Jones:

> If you know the truth then why do you care? With all the media attention this is only going to get worse for you. Your lawyer is trying to make a name for himself using you as his pawn. If anything me just seeing your face on the news right now will get you fired from your job. All you had to do is read the FAQ section like every other normal person to get stuff removed. You dug your own grave here Sarah. I am a very reasonable person ... hope it was worth it.nik.

He also removed the first three posts regarding Jones. The posts on www.TheDirty.com humiliated Jones, allegedly undermining her position as an educator, her membership in the Cincinnati BenGals, and her personal life.

Jones amended her action to proceed against [the proper defendants], alleging claims of defamation, libel *per se,* false light, and intentional inflection of emotional distress. [The case proceeded as summarized above.]

II.

A.

We review a district court's denial of a motion for judgment as a matter of law or a renewed motion for judgment as a matter of law *de novo.* ...

B.

[The court summarized the extensive caselaw according with *Zeran*'s interpretation of § 230.]

By barring publisher-liability and notice-liability defamation claims lodged against interactive computer service providers, § 230 serves three main purposes. First, it "maintain[s] the robust nature of Internet communication and, accordingly, ... keep[s] government interference in the medium to a minimum." [*Zeran*, 129 F.3d] at 330. Second, the immunity provided by § 230 protects against the "heckler's veto" that would chill free speech. Without § 230, persons who perceive themselves as the objects of unwelcome speech on the internet could threaten litigation against interactive computer service providers, who would then face a choice: remove the content or face litigation costs and potential liability. Third, § 230 encourages interactive computer service providers to self-regulate. ...

The protection provided by § 230 has been understood to merit expansion. Congress has extended the protection of § 230 into new areas. *See* 28 U.S.C. § 4102(c)(1) (providing that U.S. courts "shall not recognize or enforce" foreign defamation judgments that are inconsistent with § 230). And courts have construed the immunity provisions in § 230 broadly. Moreover, "close cases ... 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." *Fair Hous. Council of San Fernando Valley v. Roommates. Com, LLC*, 521 F.3d 1157, 1174 (9th Cir. 2008) (en banc).

Section 230(c)(1)'s grant of immunity is not without limits, however. It applies only to the extent that an interactive computer service provider is not also the information content provider of the content at issue. An "information content provider" is defined 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(f)(3). A website operator can simultaneously act as both a service provider and a content provider. If a website displays content that is created entirely by third parties, then it is only a service provider with respect to that content—and thus is immune from claims predicated on that content. But if a website operator is in part responsible for the creation or development of content, then it is an information content provider as to that content—and is not immune from claims predicated on it. Thus, a website may be immune from liability for some of the third-party content it publishes but be subject to liability for the content that it is responsible for as a creator or developer. In short, immunity under the CDA depends on the pedigree of the content at issue. ...

C.

This case turns on how narrowly or capaciously the statutory term "development" in § 230(f)(3) is read. ...

... Decisions from our sister circuits ... provide a workable measure of "development" that not only preserves the broad immunity the CDA provides for website operators' exercise of traditional publisher functions but also highlights the limited circumstances under which exercises of those functions are not protected. The leading case is *Roommates.* There, the Ninth Circuit sitting *en banc* discussed the meaning of "development" at length.. In *Roommates,* as a condition for using an online roommate-finding service, a website required each user seeking to offer living space to create a profile describing his desired roommate and, in so doing, required that user "to disclose his sex, sexual orientation and whether he would bring children to a household." *Id.* at 1161. The website also encouraged its users to provide additional comments describing themselves and their desired roommate. The fair housing councils of San Fernando Valley and San Diego sued, alleging that the website violated the Fair Housing Act and state housing discrimination laws. The court held that a website operator was not entitled to immunity with respect to allegedly unlawful content that it *required* its users to submit and with respect to the search engine that was built on that content. But the court also held that the website was immune as to claims based on the website's encouragement that users provide additional comments, some of which were alleged to be discriminatory. To arrive at these divergent holdings, the court applied a specific measure of development:

> [W]e 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.*

521 F.3d at 1167–68 (emphasis added). A material contribution to the alleged illegality of the content does not mean merely taking action that is necessary to the display of allegedly illegal content. Rather, it means being responsible for what makes the displayed content allegedly unlawful. *Cf.* [*Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc.,* 519 F.3d 666, 671 (7th Cir. 2008)] ("Causation ... must refer to causing a particular statement to be made, or perhaps the discriminatory content of a statement. That's the sense in which a non-publisher can cause a discriminatory ad, while one who causes the forbidden content may not be a publisher."). "In an abundance of caution," the *Roommates* court gave several examples of applications of the "material contribution" test. For example:

> 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.

521 F.3d at 1169. In contrast to this example, the court observed that Roommates required subscribers to disclose information about protected characteristics as a condition of accessing its service and "designed its search and email systems to limit the listings available to subscribers based on sex, sexual orientation and presence of children." *Id. at* 1166, 1169. Because Roommates required information about protected characteristics and engineered its search and email systems to limit access to housing listings based on those protected characteristics, the court held that the website materially contributed to the alleged illegality of hiding certain listings.

The court also gave specific examples of the application of the material contribution test for a website that solicits, edits, and displays content originating from third parties (*i.e.,* a website akin to www.TheDirty.com). For example:

> 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.

Id. at 1169; *see also* [*Batzel v. Smith,* 333 F.3d 1018, 1035 (9th Cir. 2003)] (holding that an editor of an email newsletter who received and published allegedly actionable information, adding a short headnote, was immune under § 230 because an editor's changes to the length and spelling of third-party content do not contribute to the libelousness of the message). The *Roommates* court further explained:

> And any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online is perforce immune under section 230. But if the editor publishes material that he does not believe was tendered to him for posting online, then he is the one making the affirmative decision to publish, and so he contributes materially to its allegedly unlawful dissemination. He is thus properly deemed a developer and not entitled to CDA immunity.

521 F.3d at 1170–71.

Accordingly, the *Roommates* court held that § 230 barred the fair housing councils' claims grounded on the allegedly discriminatory statements displayed through Roommate's operation of the "additional comments" section of its website. The court explained:

> Roommate publishes these comments as written. 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. This is precisely the kind of situation for which section 230 was designed to provide immunity.

Id. at 1173–74. Furthermore, the court rejected the argument made by the fair housing councils that the website developed the allegedly illegal content displayed in the additional comments section because the website encouraged the submission of discriminatory preferences. The court reasoned that "[t]he 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." *Id.* Because "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 discriminatory content created by users," the court held that the operation of the additional comments section did

not materially contribute to the alleged unlawfulness of the content displayed on the website's comments section. *Id.*

The material contribution test has been adopted and applied by other circuits, with instructive effect. *Compare* [*Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 254 (4th Cir. 2009)] (holding that a website *did not* contribute to alleged illegality), *with* [*FTC v. Accusearch Inc.*, 570 F. 3d 1187 (10th Cir. 2009)] (holding that a website *did* contribute to alleged illegality). In *Nemet,* Nemet, the owner of a Chevrolet dealership, sued Consumeraffairs.com, a website allowing users to comment on the quality of goods and services, after various allegedly tortious, third-party posts appeared on the website relating to automobiles sold or serviced by him. The website claimed immunity under the CDA. Nemet responded that the website was, in fact, an information content provider under § 230(f)(3), and was thus liable as a co-developer, because of the "structure and design of its website" and because "Consumeraffiars.com solicit[ed] its customers' complaints [and] steered them into specific categor[ies]." *Id.* at 256 . The panel affirmed the district court's grant of the website's motion to dismiss because "[e]ven accepting as true all of the facts Nemet pled as to Consumeraffairs.com's liability for the structure and design of its website, the amended complaint does not show, or even intimate, that Consumeraffairs.com contributed to the allegedly fraudulent nature of the comments at issue." *Id. at 257* (internal quotation marks omitted).

In *Accusearch,* Accusearch operated a website that sold the confidential information of individuals, including their telephone records, which the website paid researchers to obtain. The Federal Trade Commission brought suit against the website operator to curtail its sale of confidential information and to disgorge its profits from the sale of information in telephone records. Accusearch claimed immunity under the CDA, arguing that it merely displayed the allegedly illegal conduct that originated from its third-party researchers. The panel rejected this argument and held that the website operator developed the confidential telephone records within the meaning of the CDA. The panel cited *Roommates's* material contribution test and found "[t]hat language applies to Accusearch's role in this case." *Id* . at 1200. The *Accusearch* panel reasoned that "[b]y paying its researchers to acquire telephone records, knowing that the confidentiality of the records was protected by law, it contributed mightily to the unlawful conduct of its researchers." *Id.* The panel noted that "the offensive postings were Accusearch's *raison d'etre* and it affirmatively solicited them." *Id.* It thus found that "Accusearch's actions were not 'neutral' with respect to generating offensive content; on the contrary, its actions were intended to generate such content." *Id.* at 1201. Accordingly, the panel held that "Accusearch is not entitled to immunity under the CDA." *Id.* ...

D.

Consistent with our sister circuits, we adopt the material contribution test to determine whether a website operator is "responsible, in whole or in part, for the creation or development of [allegedly tortious] information." 47 U.S.C. § 230(f)(3). And we expressly decline to adopt the definition of "development" set forth by the district court.

The district court read the foregoing decisions, identified *Roommates* as the guiding precedent, but derived a different rule. In its memorandum opinion explaining the denial of Dirty World's and Richie's Rule 50 motion, the district court gave two formulations of a rule providing when the CDA does not bar a plaintiff's claim. First, the district court said that a "website owner who intentionally encourages illegal or actionable third-party postings to which he adds his own comments ratifying or adopting the posts becomes a 'creator' or 'developer' of that content and is not entitled to immunity." Second, in

a different formulation, the district court said that "if ... [website] owners, as in the instant case, invite invidious postings, elaborate on them with comments of their own, and call upon others to respond in kind, the immunity does not apply." ...

We do not adopt the district court's encouragement test of immunity under the CDA. The district court misapprehended how other circuits, particularly the Ninth Circuit in *Roommates,* have separated what constitutes "development" in § 230(f)(3) from what does not. The district court elided the crucial distinction between, on the one hand, taking actions (traditional to publishers) that are necessary to the display of unwelcome and actionable content and, on the other hand, responsibility for what makes the displayed content illegal or actionable. This is the distinction that divides the holdings in *Roommates* and *Accusearch,* which stripped the respective defendants of the CDA's protection, from the holdings in *Roommates, Chicago Lawyers' Committee, Johnson, Batzel, Nemet,* and *Zeran,* which barred the respective plaintiffs' claims. In *Roommates,* the website was responsible for the alleged discrimination by requiring users to submit protected characteristics and hiding listings based on those submissions. In *Accusearch,* the website was responsible for the illegal purchase and resale of confidential telephone records. But in *Chicago Lawyers' Committee* and *Nemet*, for example, the website operators provided a forum for user posts, did not require users to violate the law as a condition of posting, did not compensate for the posting of actionable speech, did not post actionable content themselves, and therefore were not responsible for the actionable speech that was displayed on their websites. The district court's rule does not neatly divide these cases. An encouragement theory of "development" does not obviously capture what was allegedly unlawful about the design of Roommate's website, particularly its search engine, or Accusearch's payment for unlawful conduct. And it does not obviously leave out the neutral fora created by the commercially oriented websites targeted by the claims in *Chicago Lawyers' Committee* and *Nemet* (craigslist.com and www.consumeraffairs.com, respectively).

More importantly, an encouragement test would inflate the meaning of "development" to the point of eclipsing the immunity from publisher-liability that Congress established. Many websites not only allow but also actively invite and encourage users to post particular types of content. Some of this content will be unwelcome to others—*e.g.,* unfavorable reviews of consumer products and services, allegations of price gouging, complaints of fraud on consumers, reports of bed bugs, collections of cease-and-desist notices relating to online speech. And much of this content is commented upon by the website operators who make the forum available. Indeed, much of it is "adopted" by website operators, gathered into reports, and republished online. Under an encouragement test of development, these websites would lose the immunity under the CDA and be subject to hecklers' suits aimed at the publisher. Moreover, under the district court's rule, courts would then have to decide what constitutes "encouragement" in order to determine immunity under the CDA—a concept that is certainly more difficult to define and apply than the Ninth Circuit's material contribution test. Congress envisioned an uninhibited, robust, and wide-open internet, but the muddiness of an encouragement rule would cloud that vision. Accordingly, other courts have declined to hold that websites were not entitled to the immunity furnished by the CDA because they selected and edited content for display, thereby encouraging the posting of similar content. We do the same.

The district court also suggested that when an interactive computer service provider adds commentary to third-party content that "ratifies or adopts" that content, then the provider becomes a "creator" or "developer" of that content and is not entitled to the CDA's protection. An adoption or ratification theory, however, is not only inconsistent

with the material contribution standard of "development" but also abuses the concept of responsibility. A website operator cannot be responsible for what makes another party's statement actionable by commenting on that statement *post hoc.* To be sure, a website operator's previous comments on prior postings could encourage subsequent invidious postings, but that loose understanding of responsibility collapses into the encouragement measure of "development," which we reject. As other courts have recognized, the adoption theory of "development" would undermine the CDA for the same reasons as an encouragement theory.

III.

We now apply the material contribution measure of "development" to the facts of this case. Jones's defamation claims target the statements that were posted by a third party on October 27 and December 7, 2009. Because Dirty World and Richie did not materially contribute to the illegality of those statements, the CDA bars Jones's claims.

Dirty World and Richie did not author the statements at issue; however, they did select the statements for publication. But Richie and Dirty World cannot be found to have materially contributed to the defamatory content of the statements posted on October 27 and December 7, 2009, simply because those posts were selected for publication. Nor can they be found to have materially contributed to the defamatory content through the decision not to remove the posts. The CDA expressly bars "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." [*Zeran*, 129 F.3d at 330.]

Unlike in *Roommates,* the website that Richie operated did not require users to post illegal or actionable content as a condition of use. Nor does the name of the website, www.TheDirty.com, suggest that only illegal or actionable content will be published. Unlike in *Accusearch,* Richie or Dirty World did not compensate users for the submission of unlawful content. The website's content submission form simply instructs users to "[t]ell us what's happening. Remember to tell us who, what, when, where, why." The form additionally provides labels by which to categorize the submission. These tools, neutral (both in orientation and design) as to what third parties submit, do not constitute a material contribution to any defamatory speech that is uploaded.

Further, Richie's comment on the December 7 post—*viz.*, "Why are all high school teachers freaks in the sack?"—although absurd, did not materially contribute to the defamatory content of the statements uploaded on October 27 and December 7, 2009. Richie's remark was made after each of the defamatory postings had already been displayed. It would break the concepts of responsibility and material contribution to hold Richie responsible for the defamatory content of speech because he later commented on that speech. Although ludicrous, Richie's remarks did not materially contribute to the defamatory content of the posts appearing on the website. More importantly, the CDA bars claims lodged against website operators for their editorial functions, such as the posting of comments concerning third-party posts, so long as those comments are not themselves actionable.

To be sure, Richie was an information content provider as to his comment on the December 7 post. But Jones did not allege that *Richie's* comments were defamatory. And the district court did not hold that Richie's comments were themselves tortious. Rather, the court concluded that those comments "effectively ratified and adopted the defamatory third-party post" and thereby developed the defamatory statements, thus ruling that the CDA did not bar Jones's claims. The district court's adoption or ratification test, however, is inconsistent with the material contribution standard of "development" and, if estab-

lished, would undermine the CDA. Therefore, Dirty World and Richie did not develop the statements forming the basis of Jones's tort claims and accordingly are not information content providers as to them.

Because (1) the defendants are interactive service providers, (2) the statements at issue were provided by another information content provider, and (3) Jones's claim seeks to treat the defendants as a publisher or speaker of those statements, the CDA bars Jones's claims. Given the role that the CDA plays in an open and robust internet by preventing the speech-chilling threat of the heckler's veto, we point out that determinations of immunity under the CDA should be resolved at an earlier stage of litigation.[4] *See Nemet*, 591 F.3d at 254 ("[I]mmunity is an *immunity from suit* rather than a mere defense to liability [and] is effectively lost if a case is erroneously permitted to go to trial.").

IV.

We note that the broad immunity furnished by the CDA does not necessarily leave persons who are the objects of anonymously posted, online, defamatory content without a remedy. In this case, Jones conceded that she did not attempt to recover from the person(s) whose comments Richie elected to publish. She conceded that she did not attempt to subpoena Richie or Dirty World to discover who authored the defamatory posts. Instead, she sued Dirty World and Richie. But, under the CDA, Jones cannot seek her recovery from the online publisher where that publisher did not materially contribute to the tortious content. Congress envisioned a free and open internet, and the immunity provision of § 230(c)(1), which subverts common-law publisher-liability, serves that purpose. While some exercises of the considerable freedom that Congress allowed online publishers are regrettable, freedom and its uses are distinct. Congress enacted § 230(c)(1) to preserve a free internet, and that enactment resolves this case.

For the foregoing reasons, we vacate the judgment in favor of Jones and reverse the district court's denial of Dirty World's and Richie's motion for judgment as a matter of law with instructions to enter judgment as a matter of law in their favor.

Questions

1. *Dirty World* argues that Section 230 "encourages interactive computer service providers to self-regulate." How effectively was Dirty World self-regulating? Should Section 230 only apply to services that act in good faith?

2. After *Dirty World*, can a website pay its contributors while retaining the protection of Section 230? Can it refuse to delete defamatory posts unless the victim pays a $250 "arbitration filing fee?" Can it delete users' posts praising a person while leaving up posts attacking that person? Can it be dedicated entirely to user-submitted content attacking a specific person (e.g. DefameMonica.com)?

3. Xcentric Ventures operates the Ripoff Report website, which actively solicits negative comments on businesses. Unsurprisingly, it is a frequent Section 230 litigant. As one court described it:

> The business practices of Xcentric, as presented by the evidence before this Court, are appalling. Xcentric appears to pride itself on having created a forum for defamation. No checks are in place to ensure that only reliable information

[4] Certification of the interlocutory appeal sought by Dirty World and Richie could have obviated the need for the second trial. An even earlier interlocutory appeal would have resolved the case prior to trial.

> is publicized. Xcentric retains no general counsel to determine whether its users are availing themselves of its services for the purpose of tortious or illegal conduct. Even when, as here, a user regrets what she has posted and takes every effort to retract it, Xcentric refuses to allow it. Moreover, Xcentric insists in its brief that its policy is never to remove a post. It will not entertain any scenario in which, despite the clear damage that a defamatory or illegal post would continue to cause so long as it remains on the website, Xcentric would remove an offending post.

Giordano v. Romeo, 76 So.3d 1100, 1102 (Fla. App. Ct. 2011) Is this an ethical business model? Is it good for society to have websites like this one? Should the law protect them?

4. Professor Garfield's weblog has a comments section. If someone posts a comment that Dean Gladstone is an arsonist, can Professor Garfield be liable for defamation? What if he holds comments for moderation and allows them to be posted only after examining them? What if he doesn't personally look at the comments, but instead feeds them through an automated anti-spam filter?

5. Was Richie's message to Jones that "seeing your face on the news right now will get you fired from your job" a threat? The phenomenon that lawsuits to keep secrets or protect privacy can cause the information to be even more widely publicized on the Internet is often known as the "Streisand effect." The singer (in)famously sued a photographer who took photographs of her home from a plane. Before the suit, the photographs had been viewed six times, twice by Streisand's lawyer. But the high-profile lawsuit by a celebrity, together with extensive criticism by Internet commenters, brought them to the attention of hundreds of thousands of people. Is the Streisand effect a positive or a negative development in media culture? Does it change how you would proceed if you were representing Jones?

Doe v. MySpace, Inc.

474 F. Supp. 2d 843 (W.D. Tex. 2007), *aff'd* 528 F.3d 413 (5th Cir. 2008)

Sparks, 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.

---

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

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.

... Plaintiffs' Verified Complaint ... 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. ...

A. Communications Decency Act of 1996 ...

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 distinguis [*Zeran* and other cases following it] 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

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

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 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). *Id.* 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 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 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 ob-

scene, 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). ...

Questions

1. Explain what the following sentence from *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 other causes of action are now preempted?

2. Without Section 230, would Facebook be viable? Wikipedia? Google? Is Section 230 a recognition of the difficult job Internet intermediaries face? A subsidy to encourage the development of the Internet?

3. Note that *MySpace* draws on 230(c)(2) as well as on 230(c)(1). What does this add to the analysis? How do the two of them fit together? How is it that 230(c)(2), which on its face protects intermediaries for decisions to *remove* harmful content, ends up helping to protect MySpace when it *failed* to remove harmful content?

4. As *MySpace* shows, plaintiffs who try to plead around Section 230 usually lose—but not always. In *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096 (9th Cir. 2009), the plaintiff alleged that her ex-boyfriend posted nude photographs of her to Yahoo!, that Yahoo!'s Director of Communications promised to "personally walk the statements over to the division responsible for stopping unauthorized profiles and they would take care of it," and that the photographs remained on Yahoo! for two months after the promise. The Ninth Circuit held that Barnes's claim for promissory estoppel survived Section 230, writing, "Contract liability here would come not from Yahoo's publishing conduct, but from Yahoo's manifest intention to be legally obligated to do something, which happens to be removal of material from publication." Is this distinction persuasive? Is it a good idea? Should Ken Zeran have pleaded promissory estoppel?

5thWheel Problem

You are the general counsel to 5thWheel, a "peer-to-peer, crowdsourced, DIY, bottom-up, artisinal small-batch ride-sharing website." The 5thWheel website lets car owners post short descriptions of trips they're planning to make, including starting point and destination and approximate time. Users of the site can browse and search the list of trips. If they find a car owner who's going their way, they can "reserve a seat" by clicking a button and entering their credit-card details. The prices are automatically calculated by 5thWheel based on the distance and time of day. The driver gets 80% of the price; 5thWheel takes a 20% commission. If there is any dispute over no-shows, 5thWheel customer service agents get in touch with the driver and passenger to sort out what happened and issue a refund, if appropriate.

5thWheel posts drivers' descriptions of their trips exactly as submitted. It arranges them within a carefully-developed taxonomy to make for easy browsing. The site is first

---

[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.

divided into different cities: so far, 5thWheel operates in 25 cities across the United States. The trips are then broken down by neighborhood, and then sorted by the time at which they will take place. 5thWheel determines which neighborhoods to classify a trip with by examining the start and end addresses supplied by the user, and it requires the user to select the starting time using a drop-down date-and-time widget.

5thWheel has received a cease-and-desist letter from the St. Louis Metropolitan Taxicab Commission, alleging that it is operating an unlicensed transportation service. Specifically, a local ordinance requires any person who "provides passenger transportation services for a fee or other valuable consideration" to have a license from the Commission. It is a misdemeanor punishable by up to three months' imprisonment and a fine of $500 per violation to sell rides without a license.

5thWheel's CEO has informed you, in an impassioned tirade, that it would be "impossible" to obtain licenses in every city for which 5thWheel has a ride board. For one thing, she explains, local taxi and limousine companies would fight it tooth and nail to prevent the competition. For another, the administrative expense of satisfying dozens of cities' wildly diverse licensing rules would make 5thWheel's business model unprofitable unless it took a much larger commission—which, of course, would drive away drivers. The whole point of 5thWheel, she finished, is to "route around inefficient local bureaucracies and that obsolete stick-your-arm-out model of getting from point A to point B." She has asked you to draft a response letter to the Commission arguing that 5thWheel is protected by Section 230. What arguments will you make, what responses do you expect from the Commission, and how will you reply?

Section 230 Reform Problem

You are on the staff of the Senate Judiciary Committee. Senator Aykroyd (R-NE), who is upset at the level of "filth and abuse" on the Internet, has introduced a bill that would replace paragraph (c)(1) of Section 230 with the sentence, "A provider of an interactive computer service shall be treated as a publisher of any information transmitted by means of the service." Senator Radner (D-NJ), who believes that free speech needs to be balanced with protections from harassment, has introduced a competing bill that would amend paragraph (c)(1) by adding to the end an additional clause that would read, "except where the provider or user has encouraged the creation of the information."

You work for Senator Curtin (R-VA), who would like your opinion on whether these measures to limit Section 230 are a good idea. He would like to encourage vibrant free speech online, encouraging online innovation and commerce, to give the victims of online attacks meaningful legal recourse, and as far as possible to improve the quality of online discourse by limiting the spread of truly noxious and harmful content. But he freely admits that he has not followed the state of Section 230 caselaw or the policy debates over it, so he is unsure what reforms, if any, would make sense.

Senator Curtin would like to know what effect, the Aykroyd and Radner bills would have on the state of the law. Are there any precedents under Section 230 that would come out differently under the proposed bills? Should Senator Curtin support the Ackroyd bill? The Radner bill? Should he oppose them both? Or should he introduce a bill of his own to amend Section 230? If you recommend the latter, provide him with draft text.