

Internet Law

Professor Grimmelmann

Final Exam - Fall 2007

I was very happy with your exams. Most showed a good understanding of the fundamental legal points I was trying to convey in this course. Many of your answers went well beyond, displaying a good grasp of the law, close factual analysis, and creativity in finding legal solutions to your clients' legal problems. You were an excellent class, and the grade profile reflects your hard work.

I graded the three issue-spotting questions by creating a twenty-item checklist. You got a point for each item (e.g. "Only Beaufort, not Megalomaniac, could sue for a GPL violation.") you dealt with appropriately. I gave out frequent bonus points for creative thinking, particularly nuanced legal analyses, and good use of facts. I occasionally subtracted a point for a significant mistake (e.g. an egregious misstatement of the applicable legal test). I graded the essay question on a scale with its midpoint at 10. The marks on your exams don't directly correspond to these scores. Instead, they're comments I made as I was reading—check marks for good points, question marks for things that made me raise my eyebrows, and so on.

After I added your blog assignment scores and your scores on the exam questions, I drew cut lines such that scores that got different letter grades were separated by at least two points, and usually more. Each third-of-a-letter-grade region was approximately five points wide.

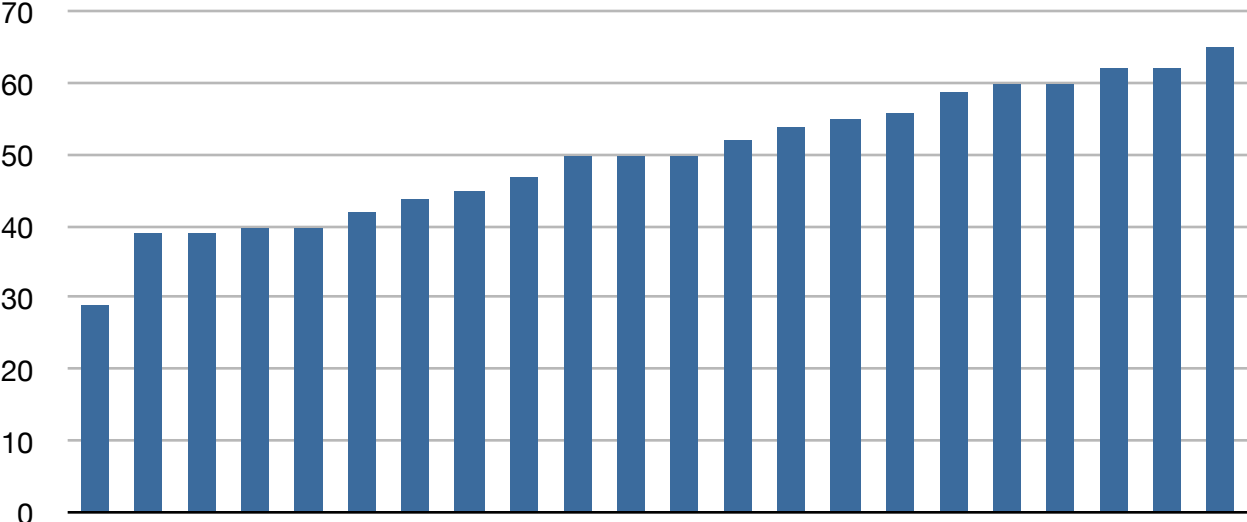
The exams are available for pickup from my faculty assistant, Bridgette Johnson, in room 706 of 40 Worth St. I'm more than happy to make an appointment with you to discuss your exam, but please read through the marked-up copy and this exam memo before getting in touch.

It's been a pleasure and an privilege to teach you. May you enjoy the best of luck in your future endeavors!

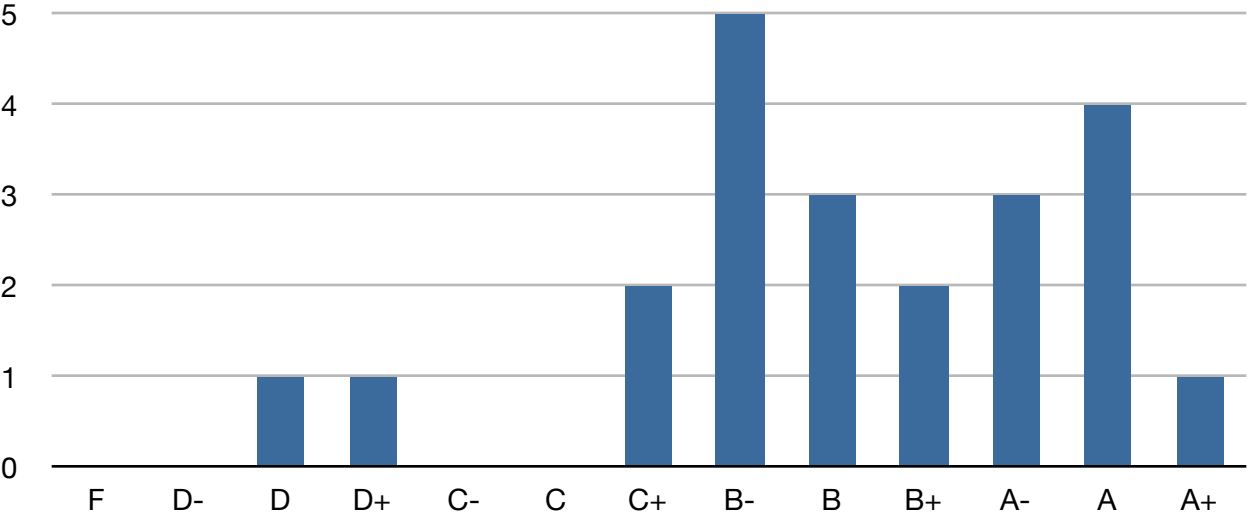
James

	Perfect Copy	Desktop Dance	Web Site	Ancient History
Mean	13.6	14.9	11.0	10.5
Median	12	15	11.5	10.5
Std. Dev.	4.4	2.6	3.0	3.3

### Raw Exam Scores



### Overall Course Grades



## (1) **The Perfect-Copy Storm**

This was the most complicated question, including a novel and potentially confusing peer-to-peer network made up of two different kinds of programs. It was also almost entirely a copyright question, and that's the most intricate body of law we studied this semester. In general, I was very happy with the organization of your thinking and your answers; you all set up your answers and worked through the issues you saw cleanly. Excellent answers distinguished themselves from "merely" good answers by being more methodical, by working through the secondary liability analysis more completely, and by explaining how Francine Beaufort fit into the picture as a (non)infringer and potential ally.

Copyright analysis starts with direct infringement. I gave points for spotting that there's a *Netcom* issue with respect to individual users, who may not know that their computers are being used to share copies. That issue could make it hard to sue individual users. It's inarguable, however, that under *MAI* there are unauthorized copies being made, so it seems fair to conclude that either the users are direct infringers or Tamiko Fujita is. (In real life, this issue could be very complicated, since we'd need to distinguish Cloud.Burst users, Cloudster uploaders, and Cloudster downloaders.)

The hardest part of the problem was the contributory infringement analysis as to Tamiko Fujita. It's hard in part because there are multiple legitimate views of how *Sony* interacts with the contributory infringement analysis. I gave full credit both for treating *Sony* as defeating the imputation of constructive knowledge to certain device makers, and for treating *Sony* as an independent defense to contributory infringement for device makers. Either way, there were five bases to touch:

- 1) Setting up the contributory infringement analysis in terms of its standard elements.
- 2) Giving a good reason for concluding that Fujita does or doesn't have knowledge of the infringements, or that it doesn't matter whether she does.
- 3) Giving a good reason for concluding that Fujita has materially contributed to the infringements. (She has, because her creation of Cloudster is a but-for and proximate cause of the file-sharing.)
- 4) Explaining that *Sony* could protect Fujita as a device-maker.
- 5) Giving a good reason for concluding that Cloudster does or does not have substantial non-infringing uses.

A few of you particularly distinguished yourselves here by noticing that while Cloudster as a whole has weather-related substantial non-infringing uses, its StormSounds feature might not.

The vicarious infringement issue was, I thought, easier. There's nothing in the problem to indicate that Fujita can change what's happening on the network now; she lacks the "right and ability to control the infringing activity." Still, a number of you asserted that she had this ability because she wrote the software originally (not necessarily true) or that she could release a new version of it now (which is true, but it won't affect anyone who refuses to download the new version). A few of you, speculated that Fujita might have hidden a backdoor in Cloudster; while that's pure speculation on the facts given, it's the sort of speculation that does turn out to be true now and then. Many of you correctly noted that Fujita gets a financial benefit from each copy of Cloudster she sells; a few went above-and-beyond by flagging the question of whether it's a

“direct” financial benefit, and by suggesting the need to survey users to find out what fraction of sales were driven by the weather-sharing features versus the file-sharing ones.

I meant *Grokster*-style inducement liability to be a minor issue; I gave a point for setting it up. I wasn't expecting much more, since the problem doesn't supply specific evidence that could be used either way on Fujita's intent in creating Cloudster. From a litigator's perspective, you could reasonably conclude that it'll be hard to prove, or that it's worth exploring in the hopes of getting more direct evidence. A few particularly good answers used some of the factors discussed in *Grokster* to try to prove intent indirectly, such as the lack of filtering and the “-ster” name of Cloudster.

The principal bottom line, which most of you reached, is that there're reasonable grounds to proceed against Fujita for some form of copyright infringement.

Beaufort, however, is another matter. Good answers noted that it's theoretically possible to reach her either for facilitating infringement by writing Cloud.Burst or for having infringing “weather data” on her computer. Good answers also noted that *Sony* probably bars the former claim, while *Netcom* bars the latter. Unless you can get some evidence that Beaufort knows about and encourages Fujita's modifications, Beaufort isn't a good choice as a defendant.

Instead, Beaufort's use of the GPL makes her a potential ally. The reasoning here is that by distributing Cloud.Burst without the source code, Fujita has violated the GPL. That gives *Beaufort* the right to sue Fujita for copyright infringement. This could be, from Megalomaniac's perspective, a great solution. Your client has a plausible affinity with weather buffs (thanks to its eco-friendly principles), so siding with Beaufort in this way lets it be the good guy, while still protecting its copyrights, and all without suing its fans. The one potential hurdle is that a GPL lawsuit might end with nothing more than the Cloudster code being open-sourced.

And now for some distractions. I gave a point for noticing these issues and for resisting the temptation to follow them too far down blind allies. First, Section 512 doesn't give Beaufort and Fujita a defense. The issue is more fundamental than that they haven't appointed DMCA agents; neither of them would be sued in her capacity *as a service provider*. In 512(c), for example, consider the language “by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider.” That simply doesn't describe the liability Fujita would face as the creator of Cloudster for facilitating copyright infringement by others.

There's potentially (if just barely) a Section 1201 issue involved in whatever Cloudster does to enable other people to download DRMed (?) files from iTunes and Windows Media Player. In practice, it would be a good idea to investigate and develop further facts; on the problem as stated, there's just not enough to go on. (And note that there's no 1201 issue at all as to those files that aren't DRMed, such as MP3s people have ripped from CDs they own.) Working through the intricacies of 1201(a) and (b) doesn't yield much more insight than just saying briefly that there's a potential issue and why.

I didn't think of this problem as raising a CFAA/trespass-to-chattels issue. A couple of exams, however, did explain how Cloudster's use of users computers to store "weather data" that isn't could be a violation of one or the other. Bonus points!

Finally, there was one mistake that I consistently docked a point for making. A number of you talked about "suing Cloudster." Cloudster is a program, one that's running on many different computers. It's not incorporated, it has no address for service of process, it has no assets. You could sue Fujita for writing it, but good luck suing Cloudster itself. This distinction isn't just pedantic. If you start talking about "suing Cloudster," it's very easy to fall into the trap of thinking that there must be some central location where it could be disabled. On the problem as written, there probably isn't; remove any one Cloudster computer and the rest will keep on sharing files, as in *Grokster*. Your job would be a lot easier if there were a central server to go after. But there isn't.

**A note on the names:** The names in the problem were a play on some famous figures in meteorology: Francis Beaufort devised the Beaufort scale, used to measure wind speed, and Tetsuya Fujita devised the F-scale, which measures tornado intensity. Cloudster is very loosely based on QLOUD, a new technology that may or may not pass the *Grokster* inducement test.

## (2) Desktop Dance Party

This was designed to be a hard question: Simpsy is obviously in the wrong and Halpern obviously in the right, and yet the most immediate legal analysis seems to favor Simpsy. I hoped that you'd trust your instincts, push harder on the contract and CFAA issues, and find that there really is a way to "get back" at Simpsy. Most of you did. As a result, this question had the highest averages.

The first, and most glaring, issue is the role of the Computer Fraud and Abuse Act. At the outset, one needs to show that Halpern's computer is "protected" and that Simpsy "accessed" it. Most answers noted that "protected" is easy to show for a computer on the Internet and moved on; a few used facts found within the problem itself to show that the computer was used in interstate commerce. Access is also easy to show; it was also easy to get a bonus point for reciting the specific facts that demonstrated access. I was particularly happy with a few answers that raised *sua sponte* the issue of Simpsy's mental state; as they noted, Simpsy is like Morris in that he released a program designed to access many computers, including ones he may not even have known about.

Authorization is of course the hardest issue in most CFAA cases. Most answers discussed the three tests we went over in class, quite satisfactorily. A few got themselves confused by conflating the Cromulent Jukebox (a program) with the laptop (a computer). There's no federal law against accessing a *program* without authorization. Thus, in applying, for example, the "intended function" test, it's not the Jukebox's intended function that matters. If it were, then the CFAA could never convict anyone, because every hacker uses her own hacking programs for their intended function: hacking into computers. Better answers recognized that the intended-function test is hard to apply on these facts, because we don't know what "function" of Halpern's laptop the Jukebox is using. The "no-account" test and the *Shurgard* test are both easier to work with, and both point more unambiguously towards finding Simpsy liable.

That leaves "damage or loss," as needed for a civil CFAA claim. It's not hard to find on the facts given: the Jukebox both deleted files (damage) and made the laptop unavailable at first (loss). The \$10,000 for a computer consultant to recover the files is an appropriate measure of the damage to the files, and it easily surpasses the \$5,000 threshold. Thus, there aren't serious *Doubleclick* aggregation issues. (Nor, given the oppressive way that the Jukebox works, is there a realistic chance to opt out.)

Whenever you see a CFAA claim, you should ask if a trespass to chattels claim is keeping company with it. Here, one is. The case is distinguishable from *Hamidi* in two ways. First, there was actual damage to the computer—the deleted files. Second, the Jukebox's initial configuration—refusing to let the computer boot until Halpern "accepted"—interfered with his possessory interest in the computer. He couldn't use it to do anything at all. I didn't require you to reach this conclusion—one could, I think, try to argue with it—only to raise the *Hamidi* issue and to cite appropriate facts bearing on its resolution.

Assuming that Halpern wants to bring these claims—and it looks like he does—the problem included enough jurisdictional facts to raise the question of where he could sue. Under *ALS Scan*,

Simpsoy has reached out into New York and caused harm there through actions targeted at New York (and really, at any other state his piece of malware ends up). Your analyses of the facts in the problem suggesting this targeting and that it would make jurisdiction appropriate were particularly good. (Ironically, Simpson's inclusion of the license agreement hurts his case, since it suggests an attempt to form contracts with New York residents, and thus arguably to engage in business in New York.) There's still the matter of the choice-of-forum clause; I wanted you at least to note that if your client can avoid the contract, it solves the problem of having to litigate in Hawaii.

This brings us to the contact question, where superficial readings of the cases could lead one astray. *ProCD*, *Specht*, and *Caspi* seem to stand for the proposition that clickwrap is enforceable and browsewrap isn't. Since this contract was clickwrap, isn't it therefore enforceable?

Most of you did exactly the right thing here. You noted the problem that Halpern's putative "assent" raises for his ability to sue, and then set about finding a way to negate that assent. We spent much of a class session on just this issue, and I'm pleased that you both recognized that this was a good case for treating the "assent" as meaningless and also found other routes to defeat the contract. The essential fact here is that Halpern's laptop was unusable until he clicked his assent. You could treat that fact as making it unreasonable for Simpson to treat his click as true assent. You could say that Halpern rejected the contract with his first click, so that the offer was no longer outstanding (though this might raise the question of whether the offer was reextended). You could treat his click as the product of duress. You could point to substantively unconscionable terms, such as the flat prohibition on uninstalling. And, in the case of the choice-of-forum clause, you could point out that the forum bears no reasonable relationship to the parties or the cause of action. However you attack it, the "contract" isn't going to hold up.

There's a wrinkle here, one that pervades the entire problem. A few of you caught it and recognized its implications (though it was possible to give a good answer without noticing it). Halpern doesn't know how the Jukebox initially got on his computer. All speculations about spam, downloads, web pages, and so on are just that: speculations. It's possible that Halpern did something earlier that could be considered more effective assent; it's possible that Halpern directly installed the Jukebox himself in some other way; it's possible that Simpson put it on in some manner that was reasonable from his perspective. I appreciated a note showing appropriate caution about these unknown facts and a desire to investigate them further. One exam drew a clever analogy to *res ipsa loquitur*; if there are such facts, Simpson should be the one with the burden to produce them.

This uncertainty also has consequences for the CFAA and trespass issues. The actionable intrusion was arguably complete *before Halpern turned his computer on*. The Jukebox was already on his computer; the files might have been gone by then. This fact undercuts some possible claims of authorization or consent; Halpern could at most ratify something that had already taken place. It also explains why the "contract" is procedurally unconscionable; Halpern is being forced to bargain to regain something that's already been taken from him wrongfully. The best answers pointed out some of these consequences.

There was one last issue lurking in the problem. When Halpern Googled for a cracked password and entered “kwyjibo,” was he doing anything wrong? Here was where treating the Jukebox as a computer led some of you astray. You went on goose chases trying to see whether Halpern could have violated the CFAA by hacking into his own computer. Both Halpern and the people who ran the password cracker were presumably doing things on their own computers. I don’t see any reasonable way to claim that access to your own computer is “unauthorized.”

A better way to tackle this issue was to ask whether there was a DMCA 1201 problem. Halpern arguably circumvented a technological measure, which is a prima facie violation of 1201(a)(1). But given the way the Jukebox works, and that Halpern was circumventing a measure preventing uninstallation rather than one preventing unauthorized installation, he probably wasn’t circumventing a measure that “effectively controls access” to anything. You could argue this one the other way; I was looking for an answer that saw the 1201 issue and the “effectively controls” subissue.

**A note on the names:** The names and words in the problem were all derived from fake names and words on *The Simpsons*. In episode 4F16 (“The Canine Mutiny”), Bart gets a credit card offer for “Santos L. Halper.” I can’t track down the precise reference for “Simpsoy,” but my recollection is that it’s the name on a piece of junk mail offering them a “Simpsoy Family Tree.” In episode 3F13 (“Lisa the Iconoclast”), Ms Hoover answers an objection that “embiggen” isn’t a word by saying, “It’s a perfectly cromulent word.” And in episode 7G02 (“Bart the Genius”), Bart plays “KWYJIBO” as a Scrabble word.



### (3) **This Web Site Ain't Big Enough for the Two of Us**

This problem was the most straightforward of the three. Ironically, that meant it had the lowest average score. It was comparatively easy to get ten points by competently running through the basic defamation and subpoena duces tecum analysis. The next ten points were all based on more subtle observations; at least one person spotted each of them, but no one put together all ten. There was room to do well, and some of you did, but the scores were fairly closely bunched.

The natural place to start is with a defamation claim over the pseudonymous criticism on Houghton Online. “Crook” and “cheat” might be problematic only because they’re so general, but the claim about rotting begonias is specific, and is probably the best place to start. (Of course, if it’s true that Greenaway did supply rotting begonias, then she has no defamation case, but she does “vehemently den[y]” the charge, and at some point you have to take your client’s word.) I didn’t expect much specificity on defamation law; just a note as to which of the statements were potentially actionable. That leaves you with a potential case against at least one pseudonymous commenter (about which more in a bit).

Can Greenaway sue Houghton Online’s operator, Burbville LLC? Section 230(c)(1) is the obvious obstacle. I wanted to see a breakdown of the statute in terms of “interactive computer service,” “information content provider,” and so on. A *quick* discussion of publisher/distributor liability was also good, along with a citation to *Zeran*. I wasn’t happy with extended discussion (in some cases nearly a full page) of pre-230 caselaw; I emphasized in class that those cases were there more as background than as viable current-day law. In any event, the answer is that 230 fairly unambiguously bars suit against Burbville arising out of the defamation claim.

Or does it? The fact that Houghton Online keeps censoring everything Greenaway tries to post seems problematic. At the very least, I wanted you to point out that 230(c)(2) also appears to shield Burbville from suit for its actions in removing objectionable content, so the fact that it deletes her posts doesn’t hurt it. (I also gave you this point if you made an argument that Houghton Online has no duty to accept her speech, since it’s a non-state actor and its decisions can’t easily be challenged under the First Amendment.) But there are two ways that a clever answer could go further. You could argue that by censoring only Greenaway’s side of the conversation, Burbville becomes a speaker, not just a publisher or distributor; it is itself the source of the one-sidedness of a conversation. You could also argue that the censorship isn’t in “good faith” (there aren’t facts to prove it, but there aren’t facts to disprove it either, and I left the description of what was going on deliberately vague), which textually might defeat the 230(c)(2) immunity. Both of these arguments are stretches, but a few top answers put together a version of one of them, with appropriate cautions that it’s unlikely to succeed. (In fact, I gave a separate “giving good client advice” point to answers that were appropriately realistic about Greenaway’s limited prospects for recovery on the facts as stated.)

The spam-filtering issue works out somewhat similarly in the analysis. (I intended to keep the forum posts and the email separate in the problem; a few of you crossed the relevant facts. I didn’t directly deduct any points for doing so, as the confusion was understandable.) This was probably the weakest portion of the exams in general; no one got more than five of the seven points potentially available here.

The governing cause of action here is probably tortious interference with prospective business relations. Again, this isn't a tort class so I wasn't picky about the details (although I did give a bonus point for good use of the elements). The first thing to note was that there are *three* potential defendants: Burbville for the filtering, Grand Spam Slam for including her on the list, and the anonymous individuals who claimed she was spamming them. It's hard to make out any kind of case against Burbville, since it appears simply to have taken GSS's list as-is. With no evidence that it had any reason not to trust GSS's list, there's no malicious intent towards Greenaway, and thus no cause of action.

GSS, though, may be another story. Per *Media3*, it can be defamatory to call someone a "spammer," and thus that accusation could potentially be the occasion for a tortious interference suit. Unlike the plaintiff in *Media3*, though, Greenaway isn't a spammer. (Bonus point for the exam that took Greenaway at her word but also suggested that she check her computer and records very carefully to make sure no one else had been using her IP address to send out spam.) Another significant problem in *Media3* was that the plaintiff there didn't present evidence of damages. I hoped that you'd discuss Greenaway's lost business, due to the emails she wasn't getting; about half of you did.

That leaves one very subtle complex of issues that few of you ventured into. How does GSS's automated system affect the analysis? If all GSS does is aggregate user-submitted reports and add someone to the list when there are ten reports, it has a strong 230 defense. In that case, though, whoever submitted the false reports that Greenaway was spamming seems to be the proper defendant for a tortious interference lawsuit. One particularly evil possibility—which two of you noted—is that GSS in fact isn't complying with its stated policies and that it won't show her the details of the reports because there weren't any. If so, then GSS is a proper defendant, since it's itself the provider of the claim that she's a spammer.

A few exams ventured into *Search King* territory. This wasn't required, and it didn't always go well, but in a few cases, you nicely discussed the question of whether GSS's statements are matters of fact (and thus potentially actionable) or of opinion (and thus shielded by the First Amendment). I think the case is distinguishable from *Search King* because, as we noted when discussing *Media3*, saying that someone is a "spammer" relates to a verifiable claim about the world. I gave a bonus point for getting to the fact-opinion issue and making a plausible argument either way.

Wrapping up the above, Greenaway has tenuous legal claims against Burbville and GSS—so tenuous that they're probably not worth pursuing—but stronger claims against the pseudonymous posters and anonymous submitters to the GSS list. Getting at them will require unmasking them. ECPA doesn't provide an obstacle, since this is a purely private matter. The way to proceed is to file a John Doe suit, and *then* move for a *subpoena duces tecum* to Burbville and GSS, asking for identifying information on the posters and submitters, respectively. I wasn't a stickler about the order, as long as your discussion made clear that the identification was essential to allow a John Doe suit to proceed. I also didn't insist that you mention both Burbville and GSS; it was enough to identify one party by name. "The ISP" was insufficient; there are multiple intermediaries kicking around in the question, and one needs to be particularly precise when specifying parties to lawsuits and targets of judicial process.

The heart of the identification issue is the legal standard for granting the subpoena; my take (and generally yours, as well) is that under both *AOL* and *TMRT* this subpoena is likely to be granted. There are no other obvious prospects for getting the information, Greenaway has a good faith prima facie case of defamation, and the identity of the defendants is essential to her ability to proceed with the suit. Your discussion of the factors and tests was excellent, and this part of the question generated some bonus points for good use of factual evidence.

Finally, this left some room to discuss strategy. Many of you suggested approaching GSS directly to try to get off the spam blacklist quickly, which is the source of Greenaway's most pressing problem. That's a good idea. (In real life, many spam blacklists are too automated to answer individual requests, but they generally are willing and eager to help people figure out why they're on blacklists and to give general advice about how to get off them if you're on one mistakenly.) Some of you also suggested approaching Burbville. It's probably a good idea to try, but it might be less likely to succeed; there's a chance that there's something shady going on at Burbville, since they keep deleting Greenaway's posts. A few exams suggested contacting Burbville so it would be "on notice" of the defamation. Unless you concluded that you had a way of defeating Burbville's section 230 immunity, this step is pointless, since section 230 doesn't care about notice one way or the other.

One last pitfall. On the facts as stated in the problem, you don't have a good basis to sue Blackheart. It's possible that by learning the identity of the pseudonymous posters and submitters, you'll learn that Blackheart is behind Greenaway's troubles. It's also possible you'll learn it wasn't him. Start with a John Doe suit.

**A note on the names:** There weren't any references lurking in here. *Green-away* seems like a good name for a florist; Blackheart is a nicely Victorian villain's name, a bit like Snidely Whiplash.

#### (4) **Ancient History**

It's hard to offer good generalizations about essay questions, so I won't say much.

Your essays were about equally split between Barlow-heads and Easterbrook-niks. I was generally very happy with your willingness to take sides. The strongest essays managed to acknowledge points cutting in the other direction, but then responded to those points with good rebuttals.

The best essays interleaved their discussion of the Barlow-Easterbrook debate with a discussion of the specific features of the 1996 Act they were discussing. That is, they'd say a few sentences about the 1996 Act and its consequences, and then add a sentence or a clause relating it back to the larger debate. That made it easy to see how the discussion fit into the essay's argument. Weaker essays, on the other hand, tended to discuss some legal issue for a page, then end with a conclusory statement that "this experience shows that X was right." That kind of discussion comes across as canned and often tangential to the question asked.

The other main best practice that good answers to this question shared was a use of specific evidence. A side-by-side discussion of Judge Dalzell's and Justice O'Connor's opinions in *ACLU v Reno* worked well for some of you; another good essay drew on *Zeran* and *Roommates* to argue that 1996 and 2007 were very different eras for Internet exceptionalism. Discussion of telecom was rarer, but some essays did it very well, including one arguing that the 1996 Act was "business as usual" and another relating network neutrality to very old debates about regulation of pre-Internet media.