Santa Clara University

Internet Law
Fall 2012 Sample Answer
Prof. Eric Goldman

Question 1

Copyright in Videos

The question asked for "major" legal risks, and the uploading users' interests in their own copyrights aren't a major risk. Jalopy should include a license in its uploading agreement, and it's not difficult to do so. Even if Jalopy doesn't, its republication should be covered by an implied license.

Although user videos might infringe third party copyrights in a number of ways, let's deal only with third party music in the videos. Much of the discussion below would apply equally to other infringing elements of users' videos.

Users' inclusion of music doesn't automatically infringe. Users could make their own music, use public domain music, or even obtain proper licenses (see, e.g., Pond5.com as an example of a "stock" music service).

If users incorporate third party music without permission, publishing the music in the video should qualify as infringement of the reproduction, distribution and performance rights. Users might have a fair use defense, however. It would depend (among other things) on (1) how much of the original song/recording they took, (2) if there were reasonably available licensing options for the music, and (3) if their actions would be characterized as "commercial," because, for example, the users are chasing the $500 payoff for selected videos. Users might have a decent transformation argument, especially if the music's substance relates to their comments in some way. If the users have a fair use defense, that ends Jalopy's liability too.

Even if the videos infringe, Jalopy will say that it is not secondarily liable or, if it is, that it qualifies for 17 USC 512. Let's focus first on the videos as users initially upload them to Jalopy.

Contributory infringement/Inducement. Jalopy will claim that it lacks knowledge of the infringing music until it receives a copyright owner's takedown notice, at which point it can avoid materially contributing to the infringement by disabling/removing the video. Many of you said that generally knowing users would post infringing content was enough to constitute knowledge of infringement. This argument was expressly rejected in Veoh.

With respect to the videos made using its loaned video camera, Jalopy has materially contributed to the *video* in another key way (providing the hardware to assist its creation), although Jalopy will argue that the loaner didn't materially contribute to the infringing *music.*

I don't think it will help copyright owners to argue that Jalopy "knew" users would pick infringing music because Jalopy required the video to contain music. This mirrors an unsuccessful argument in UMG v. Veoh.

Under the same logic, I think Jalopy isn't "inducing" infringement. They are inducing video uploads, but there's nothing overt about the desire for *infringing* uploads. Some of you rejected the Grokster case because Jalopy isn't a "device." Grokster's inducement standard can apply to websites. See, e.g., Columbia v. Fung.

Vicarious Infringement. Jalopy's direct financial interest is unclear. The videos are designed to help Jalopy's marketing generally, but it's not selling the videos or even trying to sell third-party ads connected to the videos. At best, the videos are a "draw" to consumers as discussed in Napster, but the consumer draw isn't any infringing music (unlike Napster). As initially submitted, Jalopy probably lacks the right and ability to supervise the infringement; it naturally can remove content from its servers, but that alone shouldn't satisfy this prong.

Fair Use. Like its users' fair use defense, we can't easily assess the defense in the abstract. Jalopy's commercial interests are stronger than its users' because it's a for-profit company and the videos will contribute to its marketing objective, and as a repeat player Jalopy may have better access to music licensing options than its users do.

512 Defense. Assuming Jalopy satisfies 512(c)'s formalities (e.g., registering an agent with the Copyright Office), then it should have a 512 defense for users' initial video submission. Veoh makes clear that 512 can apply even if the plaintiff makes out a claim for contributory or vicarious infringement. Even if Jalopy's arguments against the prima facie case of contributory and vicarious infringement fail, those arguments should work for 512(c). The Ninth Circuit said that the identical words in a legal test can mean different things in the plaintiff's common law prima facie elements versus the defendant's statutory safe harbor.

Selected Videos. When Jalopy selects videos for its worst car mechanics page, it changes its legal posture with respect to those videos:

- Employees have reviewed the video and could have identified the music as infringing. This manual review could mean that Jalopy has actual knowledge of infringing music or, at least, red flags of infringement.
- By building a custom page around the video, copyright owners can now argue that Jalopy is no longer "storing the video at the direction of users." Instead, Jalopy is making the publication decision (this also may waive any "volitional" defense it had under Cablevision). Thus, Jalopy could expose itself to direct liability, not just secondary liability, for the selected videos. Jalopy could argue that its "worst" list is just like a "most popular" list of UGC, though typically those lists are generated automatically, not through human review.

If Jalopy deems its legal position too risky, Jalopy could give up its 512 posture for these videos and, instead, as part of its decision to embrace these videos, undertake to confirm there are no

infringing elements in the videos. After all, there are only a "few" videos that it would need to diligence.

Defamation/Privacy and 47 USC 230

Note: many of you collapsed the video recording of the mechanic with the user's self-review of the mechanic. Even if the video recording is a "fact," the user's exposition may not be.

Defamation. Users may make defamatory statements in their videos. They are required to explain why the mechanic is a bad mechanic, and in doing so, they are likely to make statements of fact. Any false statements of fact could be defamatory.

Some statements will be excused as opinions. Others may be excused under the First Amendment because they relate to matters of public concern. However, the businesses, and certainly the proprietors, may qualify as private individuals instead of public figures, so the applicable minimum scienter may be negligence, not recklessness. Where state anti-SLAPP laws apply, they may further protect users' videos by forcing plaintiffs to do a better pleading job or get tossed out of court.

In addition, Jalopy makes its own characterizations of car mechanics that could be defamatory, including applying the labels "car killers" and "worst car mechanics" to them. "Worst" is probably an opinion, not a statement of fact. Note http://www.forbes.com/sites/ericgoldman/2012/08/27/tripadvisors-dirtiest-hotels-ranking-makes-the-grade-in-court/. For that matter, "car killers" might be deemed an "opinion," and if not, it is fairly obviously rhetorical hyperbole. Compare this post about calling someone a "terrorist" as rhetorical hyperbole. http://blog.ericgoldman.org/archives/2012/12/calling_someone.htm

Privacy. Users are required to capture a conversation between the mechanic and another customer. Although the users aren't required to make the video secretly, it may be difficult to catch an honest conversation any other way (after all, people might tone down their behavior when they see the camera; or the mechanic might throw the videographer off his/her premises). Further, Jalopy helps users make surreptitious videos by loaning equipment designed for that purpose.

If the user makes the video in a "public" place, the video publication could constitute a public disclosure of private facts, such as details about the third party customer's situation. This is like capturing a person being rushed into the emergency room. Even if publicity of the mechanic's poor conduct is in the public's interest, the privacy interests of the third party customer have to be considered as well. If the video is captured in a "private" place (whatever that means in the context of a business' facility), additional privacy protections could apply to the conversation between the mechanic and the customer, plus the video could be an intrusion into seclusion. (We deliberately avoided the ECPA in the course, but there are also probably ECPA problems (see 18 U.S.C. 2511(1)(b)(iv)(A)) and state-law equivalents; and any such claims would be excluded from 47 USC 230).

A false light claim might apply if a video is misleadingly edited. Each individual snippet of video might be true, but the clips could be complied into a way that creates a false overall impression.

The mechanics and third party customers could also argue that the video violates their publicity rights, but that's a very low-merit claim because the videos fairly clearly constitute editorial content, not ads. However, the mechanics might get a little more traction when Jalopy uses the mechanic's name in the ad copy. Note that Section 230 wouldn't protect Jalopy from that publicity rights claim in most jurisdictions because it's an IP claim, but it might protect Jalopy in the Ninth Circuit.

47 USC 230. Section 230 should not apply to Jalopy's own statements, such as the "worst" and "car killers" designations, and potentially the other points I mentioned above (ECPA and publicity rights). However, presumptively Section 230 protects Jalopy from any defamation or privacy claims based on the videos' content. Jalopy qualifies as a provider of an interactive computer service, the users created the video, and any defamation/privacy claim against Jalopy would treat it as the publisher or speaker of that video. The fact that Jalopy adds content around the video doesn't change the video's character as third party content.

However, Jalopy could be vulnerable to a Roommates.com bypass to its Section 230 immunity. Jalopy may satisfy even the most narrow reading of Roommates.com's holding: that Section 230 immunity applies unless the website encourages illegal content or designs its website to require users to input illegal content. Here, the "illegal" content is the users' defamatory content or the privacy invasions. Jalopy does several things to encourage, or require, these outcomes:

- users must say derogatory things about their mechanics
- users must capture a third party customer in the video
- Jalopy will help users capture video surreptitiously through the equipment loan. Does supplying the recording equipment to users make Jalopy a partial content "developer"?
- Jalopy pays a non-trivial amount for the videos it thinks represents the worst mechanics, giving submitters a financial incentive to dramatize/fictionalize their experiences

At the same time, Jalopy never explicitly requires or encourages *illegal* content. Unlike the Roommates.com sequence of web pages, where users had to answer questions that presumptively violated the law, users' videos don't have to lie or invade privacy to publish their videos. Indeed, analogous websites like Ripoff Report and PissedConsumer have repeatedly succeeded with Section 230 defenses.

Jalopy's decision of which videos to select for additional promotion does not affect the Section 230 analysis. See Zeran. Further, Jalopy may be able to claim Section 230(c)(2) protection for those selections as well.

So long as it's third party content, the factual information added by Jalopy's employees could still qualify for Section 230 immunity even if Jalopy employees manually added it to the website. The addition of this content would not affect the Section 230 analysis for the users' videos.

Trademark

Jalopy references car mechanics' business names in at least three ways:

- URL path
- On the text of the page. The users also reference the business' name in their videos, but I'll ignore that because I think users make a purely editorial reference.
- In Jalopy's house ads

Let's assume the car mechanic has a protectable trademark in the business name. The car mechanic has priority over Jalopy. Although it's not clear if Jalopy makes a use in commerce, chances are they do. First, the overall scheme is designed to enhance Jalopy's marketing, even though some of its references are purely editorial. Second, at minimum putting a third party trademark in ad copy usually qualifies as a use in commerce.

Is there a likelihood of consumer confusion? By the time consumers reach Jalopy's page, the relationship between Jalopy and the car mechanic will be clear (and unflattering to the car mechanic). The URL references "car killer," although the slang "killed" could be misinterpreted as a laudatory statement. Jalopy's house ad is also likely entirely clear to consumers, although we'd need to see the exact implementation. It's similar to a comparative advertisement.

As a result, a car mechanic's only real trademark infringement claim is for initial interest confusion, such as Jalopy appearing in search results for the car mechanic's name (something that Jalopy is deliberately trying to do). Because I don't know how to define initial interest confusion, I can't say with confidence that Jalopy is or isn't creating it. Still, thinking broadly, we want sites like Jalopy to hold bad car mechanics accountable, and trademark law shouldn't disrupt that. As a result, I think many judges would refuse to find initial interest confusion in this circumstance. See, e.g., Ascentive, LLC v. Opinion Corp., 2011 WL 6181452 (E.D.N.Y. Dec. 13, 2011).

Many of you discussed "diversion" as part of initial interest confusion, but what does "diversion" mean—especially in a non-competitive situation like this?

Even if a car mechanic establishes a prima facie case of trademark infringement, Jalopy may have defenses, the most obvious one being nominative use. Jalopy is referencing the car mechanic's business name because that's the most effective way to describe the business, and if Jalopy only uses the name (as opposed to, say, a logo), it clearly took only what was necessary to make its point.

Dilution is an unlikely claim. First, the major auto repair chains (Midas, Jiffy Lube, Pep Boys) may have a trademark known to the general US consuming public, but most local mechanics won't. A mechanic's shop that includes a famous trademark (e.g., Joe's Honda Repair) isn't itself a famous mark. Second, Jalopy's activities probably qualify for the statutory defenses of fair use, criticism/comment or news reporting.

An ACPA claim is even less meritorious. The ACPA applies to first- and second-level domains because those are "registered by"/"assigned by" a third party service. Everything else in the URL isn't, and therefore isn't covered by the ACPA. See, e.g., Goforit Entertainment LLC v. Digimedia.com LP, 2010 WL 4602549 (N.D. Tex. Oct. 25, 2010). Further, Jalopy does not have a bad faith intent to profit *from the domain name*.

Some of you attempted to squeeze a jurisdiction issue out of these facts, but there wasn't much to work with.

Recommendations

- Complete all formalities required to satisfy 17 USC 512(c). 512(c) isn't a complete solution to Jalopy's problems, but it's worth the effort.
- Give up the 512 safe harbor for selected videos and fully vet them for copyright infringement. This takes on more risk, but increases Jalopy's control of the risk. Jalopy might get insurance to cover the risk that employees miss any infringements.
- In-line link the selected videos rather than "republishing" them. This may be form over substance, so I'm not sure how much this would help, but it invokes the distinction from the Flava Works case between in-line linking and hosting.
- Create (or link to) a library of free music samples that users can incorporate. Or obtain a license from a stock provider of music like Pond5.com. Or, Jalopy employees could add licensed music to videos after they are selected.
- Jalopy could consider using automated music infringement filters, but this may be cost-prohibitive.
- Don't encourage users to engage in surreptitious behavior. That never plays well in court.
- In particular, do not loan out digital video recorders, which seems to encourage users to capture video they aren't supposed to get. Even if Jalopy could analogize its users to investigative journalists, the potential for mischief is too great. Plus, those cameras will never be returned. On the downside, Jalopy may not be able to get candid interactions between mechanics and customers.
- Change the name "Car Killers." Even if it is rhetorical hyperbole, it's still potentially actionable. Jalopy might tone down the "worst" claim as well. On the downside, colorful characterizations do a better job advancing the marketing objectives, so expect some pushback from the marketing team.
- Remove the car mechanic's name from the ad copy. It just adds liability, and the ad copy works just fine without naming specific names.
- Consider blurring faces in the recording of the mechanics and removing/obscuring all references to the business and mechanic's names. Jalopy isn't really interested in trashing individual businesses but to show that mechanics overall are not as trustworthy as self-maintenance. However, I wonder if too much obscuring would undermine the credibility of the video?

Recommending to kill the Car Killers feature outright will not be popular with the marketing folks—another example where the lawyer just says no.

Similarly, many of you recommended kiboshing the music requirement. Can you do better than that? Music can improve the video's professionalism and overall watchability. Perhaps Jalopy could make "professional quality" one of its evaluation criteria without explicitly requiring music as one component.

Other examples of possibly over-aggressive suggestions many of you made:

- killing the video component of the reviews. Some people learn better via audiovisual content, and it can feel more authentic to have a person explain their opinion visually.
- Post both positive and negative reviews. How would allowing positive reviews advance Jalopy's business/marketing objectives?

Some of you argued that Jalopy should shift all of the legal responsibility to users in the user agreement. Although that's OK, this contractual agreement between two parties in privity usually doesn't bind third parties, so this suggestion doesn't really do much.

Question 2

I know this question looks a little different than past years' questions. I did that in part to avoid the rut of asking another scraping-style question, something we didn't emphasize quite as much as in years' past. Plus, we spent so much time talking about our feelings, I thought it would be valuable to put those on the exam.

I didn't expect you to make any specific arguments or points other than to answer the questions I asked. My "sample" answer below (which vastly exceeds your word count allotment) isn't offered as a model for your answer; rather, it's just an exposition designed to highlight some of the considerations you might have addressed.

Overall, I was happy with the heartfelt and opinionated responses I got from many of you, but I was also sad that I didn't hear more of these views in class during the semester. What can I do to make you feel more comfortable publicly airing some of the views you shared in your exam answer?

——

As a threshold matter, there are the three main players in the Internet ecosystem: a client, a server (like a website), and the entities (like Internet access providers) who carry the bits between the two. Each player owns chattels that process Internet data. If we are going to treat them differently, we ought to explain why. I'll touch on some examples of differences between these entities below.

We can break down the trespass to chattels (TTC) doctrines on three dimensions:

1) Who has the possessory interest?
2) How third parties are given notice delimiting the chattel usage
3) When does the chattel owner experience legally recognizable harm from the use?

Possessory Interest

A threshold question: who is a proper plaintiff because their possessory interests are interfered with. This may sound simple, but it often isn't. I use a laptop provided to me by the university. If my laptop is "trespassed," whose interest has been interfered with? Mine, the university, both of us, neither of us?

An even harder case is when a customer obtains cloud storage space. This can range from web hosting circumstances like my personal website (hosted on a third party service provider's computers) to the various UGC websites that provide us with accounts to publish content (YouTube, Flickr, Facebook and so on). If my YouTube account is hacked, do I have a reason to complain about trespass to chattels? (Ignore other legal issues with the hacking). Perhaps not, but we may need more facts to answer the question. I pay for storage and bandwidth for my personal website (again, the university picks up the tab; let's put that aside), so someone improperly accessing my personal website may cost me money. Should a "lessee" or "licensee" of a cloud storage provider get standing to enforce a trespass to chattels? If not, we could end up with a situation where the web host/provider is the only plaintiff but they don't care about the chattel interference as much as their customers do. Cf. the Lori Drew case, where MySpace was the purported CFAA victim when a user lied about her identity to get online and do bad things to another user.

How to Delimit Use?

From a Coasean standpoint, we should set the property allocation and then let parties bargain to their preferred outcome. So we could say that server operators have the absolute entitlement and need not give any notice of restrictions to users; users must negotiate any rights to use the server. Or, we could say that users have the absolute right to access the server, and server operators must negotiate any limitations on use. I'm torn about this initial entitlement because I favor property owner's right to exclude, but I also fear the misuse of these rights will create gotchas or pseudo-IPs.

Either approach leaves open the mechanism for bargaining, especially in light of the Internet's architecture where a server operator may be dealing with millions of users, each worth a relatively low economic amount. Requiring personalized negotiations would be overwhelming, but automated "negotiations"—via form contracts or technology—raise their own questions.

Technology provides one possible solution. We could encourage a technological arms race, where server operators take steps to lock out unwanted users, and users take steps to route around any technology controls. Whoever wins the arms race wins; no court battle required. Arms races are socially wasteful, though, so we might not want to rely on this.

Alternatively, technology could provide automated instructions to users, "negotiating" rights that way. Robot exclusion headers are one example. Currently, we don't treat robot exclusion headers, or other forms of automated instructions, as conclusive, but we could.

Instead, today we principally rely on text disclosures by server operators in user agreements and site policies to "negotiate" server usage with users. Our current approach today is probably sub-optimal. For TTC purposes, server operators can restrict users with something less than a properly formed clickthrough agreement, raising questions whether users get adequate notice of the desired restrictions. The cases we read largely side-stepped this notice issue because the user had actual notice, but in other cases imposing TTC on users based on unknown restrictions would be grossly unfair.

We may not want to require server operators to form mandatory non-leaky clickthrough agreements to obtain TTC exclusionary rights. At that point, TTC becomes co-extensive with contract law and, in some cases, the clickthrough agreement isn't possible because there's no privity (e.g., Hamidi). Still, we might want the TTC doctrines to explicitly require actual defendant knowledge of the restriction and put the burden on the plaintiff to make that showing.

Notice that this discussion holds clickthrough agreements up as the gold standard, but clickthrough agreements have also contributed to the "crisis of contract" we discussed in class. Clickthrough agreements look like a contract legally, but we don't believe people understand what they are agreeing to or really accept all of the terms. Allowing server operators to control user behavior through TTC using something less than a clickthrough only exacerbates the "crisis of contract" by enforcing terms that people didn't (by definition) agree to. Assume we don't do that, I am willing to accept the crisis of contract caused by clickthrough agreements as the "price" of otherwise socially beneficial reduced transaction costs (I'll discuss the social implications of that in a moment).

While I've focused on server operators, we might consider if the rules should be different for users' computers. Users are in a worse position than server operators to engage in a technological arms race, and users lack some of the simple technologies (like robot exclusion headers) to communicate their "deal." (I note some exceptions, like cookie settings and the emerging do-not-track standards).

Many of you advocated more highly visible notices, like unavoidable pop-ups when you first visit a website. Is that really the world you want to live in? i.e., any time you visit a new website, you must navigate legal terms and make a decision? The EU is already trying to force top-of-page disclosures regarding cookies. Imagine if we multiple the efforts to provide such visible notice. How many different issues need top-of-page disclosure, and how will we manage that? Many of us will simply develop a blindness to those disclosures, or there will be so many disclosures that they will crowd out/down the truly important ones—as well as the substantive content the user actually wants. Also, highly visible notice doesn't necessarily address the situations where there's lack of privity, like spam.

Legally Recognizable Harm

Right now, the TTC doctrines are all over the map regarding legally recognizable harm. Common law trespass to chattels in California requires harm to the servers. This standard itself is murky, as the harm could be de minimis but nevertheless actionable if the facts align themselves right, and the California Supreme Court had no principled way to explain why

Hamidi's actions didn't harm the servers (especially in light of the trial court's findings). The CFAA requires minimal harm, such as the $5k threshold, which rarely acts as a limit on actions (but did screen out the Ticketmaster CFAA claim). California Penal Code 502 effectively requires no harm at all; simply making unwanted use is its own harm. This heterogeneity of harm standards makes no sense.

On balance, I tend to favor some minimum harm thresholds as a way of screening out ridiculous claims, like the cookie lawsuits. However, I'm sympathetic to the strong property rights position, which says that chattel owners should have strong excludability over their property even if they can't show harm.

For me, the harm issue is linked to the notice issue. I'm less opposed to strong property rights if restrictions have been clearly communicated to users. If users aren't clearly told of the restrictions, I expect chattel owners to make a more persuasive showing of harm.

It was interesting how many of you expressed an anti-exceptionalist view, i.e., online trespass to chattels should be like offline trespass to chattels. But some of you took the incorrect position that offline TTC doesn't require harm, so online TTC shouldn't either. The Restatements makes it clear that offline TTC, unlike real property trespass, *does* require some harm. Recall in class I gave the example of touching a dog's ears; that's a chattel interference, but it's not actionable because there's no harm. So I was fine with the anti-exceptionalist view, but I was not impressed if you then reached the conclusion that no legally recognizable harm should be required. One or the other, please.

Social Interests

Property rights involve a balancing of interests. Real property rights are never absolute, although sometimes they are caricatured that way.

Online, we should be nervous about anything that would impose, or increase, transaction costs of bargaining (the Coase Theorem says that where there's transaction costs to bargaining over the entitlement, the best social policy is to reduce or eliminate those). The Internet has done a magical job of allowing hundreds of millions of users to interact with each other with low or zero transaction costs. We should fight to preserve this.

Ways to do this include:

- presumption that people connected to the Internet want to talk with each other, so the chattel owner has the burden to vary the default
- we should favor automated and standardized means of communicating chattel restrictions over text-communicated restrictions
- we should ignore obscurely presented chattel restrictions
- we should require aggrieved chattel owners to show some minimum quantum of bona fide harm before going to court, and that harm should be consistent across all TTC doctrines
- we should require chattel owners to engage in self-help first, i.e., show they tried to fix the problem themselves.

I might favor ignoring all text-communicated chattel restrictions unless they are communicated via a clickthrough agreement. That would effectively merge TTC into contract law, which isn't necessarily a bad thing when clickthroughs are possible. However, clickthroughs aren't always possible—see, e.g., the spam in Hamidi, or Internet access providers dealing with non-customers—so we may want a backstop legal doctrine in those circumstances rather than trying to contort contract law to bail out these chattel owners (see, e.g., the legal contortions of the contract discussions in Register.com and Ticketmaster cases).

One last thought: TTC doesn't need to solve all problems itself. It just needs to gap-full all of the other applicable doctrines, which might include breach of contract, IP claims, anti-spam laws, various computer crimes (non-TTC), trademark law, cyber-harassment, ID theft, etc., etc. Also, we should recognize that some of the gaps are filled through technological measures. Perhaps one of the biggest failings of online TTC is that we haven't figured out exactly what problems we want the doctrine to solve in light of the adjacent legal doctrines.

In reading your answers, I progressively became persuaded that TTC is a solution in search of a problem. I believe the following three approaches are all we need:

1) Chattel owners should deploy technological controls.
2) Chattel owners can use contracts (real contracts, not Register.com hacks) to control user behavior not controlled by technology.
3) In the situations where technology and contracts aren't sufficient, we should have narrow anti-hacking and DoS crimes enforceable only by prosecutors. The crimes should be subject to public policy limits (like concerns about competition), require a high level of scienter, and be precise enough to survive criminal vagueness challenges.

If we adopt these three principles, we're effectively giving users the Coasean entitlement (except for criminal hacking). The chattel owner, by connecting the chattel to the Internet, has to bargain for any restrictions via technology or contract. In effect then, I think the TTC doctrines may be unnecessary.

In grading this question, things I looked for included:

- your personal reactions
- internal consistency of your positions
- answers to both the TTC and contract/notice piece
- considering different factual circumstances, such as the spam situation when there's no web interface and no privity
- points that were more than just platitudes. Some of you led up to your grand conclusion that it's bad for people to do something "unauthorized" or "improper." I can't argue with that, but the key issues are what makes something "unauthorized" or "improper," and if you didn't take it that next step, I didn't get much out of your answer.

Some of you seemed to conflate TTC with data privacy, treating data as the "chattel." This made for highly confusing answers.

Tips for Students

- *Always* get the client name right. Some of the variations I saw: Japlopy, Jalope, Joply, Jaolopy, Jolopy
- Listen to your emotions, but don't give into them. Some of you had such a strong negative reactions to Jalopy that you twisted the legal doctrines to make sure Jalopy would go down. That may be the right result, but the exam requires you to analyze the doctrines with a level head. After you've done that, I want to hear your emotional response too.
- I can no longer accept wrong answers on 47 USC 230. For example, Section 230 doesn't go away just because Jalopy exercises editorial control over user submissions. I don't know how I failed to make that clear from class, and outright misunderstandings of a key doctrine from class hurt your score. Further, Roommates.com is an exception to the general Section 230 rule, but it's a weak one. Jalopy might very well fit a Roommates.com exception, but you should be quite precise about why that's the case. Simply treating Roommates.com as a general catch-all exception to Section 230 is incorrect.
- I saw similar problems with Grokster. Remember: Grokster is the exception to the rule, so use it precisely.
- Some thoughts on how you could have improved your score:
    - Answer all of the questions asked
    - Address all of the key issues (i.e., in Q1, copyright, trademark, privacy, defamation and Section 230). I was shocked that some of you didn't mention Section 230 ONCE in your exam. If you write an Internet Law exam in a class taught by Eric Goldman and you don't mention Section 230, *you are doing something wrong*. A surprising number of you didn't discuss trademark in Q1.
    - Use the scattegories approach to your proactive recommendations—cover both the obvious suggestions AND come up with some original/distinctive suggestions. See http://blog.ericgoldman.org/personal/archives/2007/06/law_school_take.html.