Santa Clara University

Cyberspace Law Final Exam Sample Answer
Fall 2008
Professor Eric Goldman

Once you got past Q1's weird facts, as you'll see, this was a pretty easy exam. There were 9 As, 22 Bs and 8 below-Bs.

QUESTION 1 (mean word count of 1889)

Liability to Target Websites

There were three main points I wanted you to discuss in this section: copyrights, contracts and trespass to chattels (and related doctrines). If you omitted one or more of these three doctrines, your score suffered accordingly.

I also wanted you to distinguish Hornblower's direct liability from her derivative liability for her readers' behavior. If you were able to segregate these issues nicely, especially on the trespass to chattels/contracts discussion, you generally earned extra points (but this could have been overwhelmed by missing a key doctrine).

Hornblower's art project looks a lot like a distributed denial-of-service (DDOS) attack. We didn't discuss DDOSs directly, although the facts do look *a lot* like the Ticketmaster v. RMG case. Frankly, I was surprised that more of you did not discuss or cite the case, especially because we spent about a full class session using the case to review the first half of the semester. In retrospect, if you didn't connect this fact pattern to the Ticketmaster case, you're probably now realizing how easy this question was.

I would break the answer into two parts: Hornblower's configuration visit and the applet's subsequent accesses.

<u>Hornblower's Configuration Visit</u>

To identify a website to target, Hornblower inevitably would visit the site, raising the following issues:

- *Copyright*. By browsing the site, Hornblower makes copies of the web pages. If the web pages contain any copyrighted material owned by the website operator (almost certain to be the case), Hornblower creates a prima facie case of copyright infringement by downloading the page into her RAM and perhaps into her cache. See Cablevision, Perfect 10 and Ticketmaster. Because this is an "ordinary" visit, Hornblower's browsing should be excused under fair use, implied license or both. If her computer doesn't retain a copy of the page, it's also possible that the copy isn't sufficiently fixed (Cablevision).

- *Browsewrap*. If Hornblower visits only a single page on the target website, then it would be impossible for her to be bound to any contract terms because her actions do not unambiguously manifest assent. If she browses around the site, in theory she might bind herself to the browsewrap, but only if her browsing manifests assent. Such a browsewrap could also destroy any implied copyright license to browse.
- *Server Restrictions.* It is implausible that a single "ordinary" web visit could be a common law trespass to chattels. In theory, such a visit could violate the CFAA or Penal Code 502 if the access was unauthorized, but as with the implied copyright license, Hornblower would have to learn of the restrictions.

Because Hornblower may never learn of any applicable restrictions on her visit, it seems unlikely that, without something more, Hornblower's configuration visit created liability for Hornblower.

Hornblower's Link to the Target Website/Readers' Use of the Applet

Copyright

It is not clear if Hornblower or her readers are "responsible" for the copies made by the applet as it requests the target website's home page multiple times a minute. Hornblower can argue that her readers' computers are requesting the copy and therefore she is, at most, derivatively liable. Her readers can argue that their computers are only following the instructions embedded in the applet, and therefore they are not acting volitionally. Hornblower can counterargue that her readers voluntarily downloaded the applet knowing what it would do, and therefore it is their choice, not hers. In some sense, this mirrors the debate about who recorded copies on Cablevision's servers. In that case, the court said the users "pressed the button" and made the copies. In this circumstance, I'm not sure what a court would do.

If the users are making the copies, then as with Hornblower's browsing, they commit a prima facie case of copyright infringement. (If not, this analysis applies to Hornblower instead). It's possible for the reader to claim no fixation if the facts could support that. Otherwise, unlike Hornblower's initial browsing to review a target website, the defenses may not be as availing. While an implied license might permit "normal" browsing, courts may be less willing to find an implied license for heavy automated browsing. With respect to fair use, the copies are the consequence of part artistic project and there is no marketplace cannibalization for the copyrighted works (although server disruption could act as a marketplace hindrance, especially for ad-supported sites), so superficially the analysis might point in favor of fair use. However, from an equitable standpoint, courts would be reluctant to condone a DDOS-like attack, so I expect most courts would skew against fair use here (just like Ticketmaster did).

Assuming that the reader is the direct infringer (instead of Hornblower), then Hornblower is probably contributorily liable for the readers' infringement. Hornblower clearly has the requisite knowledge that readers will access the target website's page because she configures the applet to do so and links from her site to the target website. By configuring the applet, she also *causes* the infringement to occur. ("Causes" is an alternative to "materially contributes.") Alternatively, Hornblower induces the infringement by distributing the applet encouraging users to use it to commit infringement (Grokster). However, Hornblower is not likely to be vicariously liable;

even if she has the requisite supervisory power, she appears to lack any direct financial interest in the infringement.

Breach of Contract (Browsewrap)

As discussed above, it is unlikely that Hornblower formed a binding contract during her configuration visit. As a result, if she is responsible for the applet's operations, she is not likely to breach a contract formed during her configuration visit (because none formed). It's also unlikely that her operation of the applet forms a new contract with the target website because she never personally revisits the target website. However, under Register.com v. Verio, she could form a contract by continuing to take the benefits (causing the applets to repeatedly visit the site) knowing of applicable restrictions—if she ever learns of the applicable restrictions. It's not clear when she would learn of these. She might have learned them if she actually looked at the browsewrap on her configuration visit. She could also learn the restrictions if a target website communicates them to her after-the-fact, such as through a C&D. Otherwise, Hornblower is probably not in breach of contract.

If readers are responsible for the applet's activities instead of Hornblower, then the target website faces the same problem binding them to a contract. A reader's visit to a single web page shouldn't form a contract, and as with Hornblower, the applet's repeated function won't trigger a Register.com-style contract formation without at minimum applicable knowledge of the terms. Furthermore, from Hornblower's perspective, even if readers form a contract, it's not clear how the contract breach could be imputed back to her. Some of you tried to solve this problem with a very expansive principal-agency relationship between Hornblower and her readers, but I think the agency argument is not very tenable in such an attenuated context.

Server Usage (Common Law Trespass to Chattels/CFAA/Penal Code 502)

Under each of the doctrines, the repeated website accesses by the applet and the non-functional URLs cause cognizable interference with the target website's chattel. They constitute a use of and contact with the target website's server under common law trespass to chattels. Under 1030(a)(5)(A)(i), the applet transmits information/commands to the website (both the request for the page and the bogus URL). Under 1030(a)(5)(A)(ii) and (iii) and California Penal Code 502(c)(7), the applet accesses the website by requesting the page. I think Penal Code 502(c)(3) also applies ("use" of computer services).

Once again, it's not clear whether that interference is caused by Hornblower or the readers. It makes a difference for two reasons. First, any individual reader's actions are unlikely to cause much damage to the target website, so if it's website v. individual reader, the website's claim effective evaporates. In contrast, if Hornblower is the relevant tortfeasor, then a website's claim would aggregate all of the individual readers' activity in assessing damage. Second, though there have been a few goofy cases on contributory trespass to chattels, the doctrine isn't very well-developed and therefore Hornblower might not be derivatively responsible. (As usual, the Ticketmaster opinion wasn't very enlightening on this point).

Assuming for a moment that Hornblower is responsible for the chattel interference due to her implementation of the applet, then the website would have to show the requisite damage. Under the Hamidi reading of common law trespass to chattels, the applet would need to "cause [or threaten to cause] measurable loss to computer system resources." Certainly the target website operator could point out a variety of harms—server capacity consumption, bandwidth consumption, spammed server logs, etc.—but it's not guaranteed that a website could satisfy the Hamidi standard. For that matter, the website may not be able to satisfy the more inclusive majority standard for common law trespass to chattels. It may depend on the actual server loads imposed on the website, which in turn may be a function of the number of readers who use the applet and whether they do so simultaneously.

The CFAA requires $5,000/year of loss. With a company like Intel, this is easy to find/manufacture, but it may be harder here. If the target websites are mom-and-pop gripers, it may be difficult for them to show any financial loss; and very difficult to aggregate that to $5,000. Note that even Ticketmaster (surprisingly) couldn't clear the $5,000 threshold.

California Penal Code 502 is much more flexible about damages. It appears just about any damage will qualify. Therefore, it is Hornblower's biggest risk of the three server protection doctrines.

Defamation

I wouldn't have discussed defamation in my answer, but enough of you did in yours that I want to briefly address it. In theory, the encoded message could contain an untrue factual statement. The example in the facts—the statement that the target website operator isn't "sweet"—isn't a factual statement; it's a protected opinion. Moreover, unless readers see Hornblower's message, then it may not be "published" because only Hornblower and the server operator would see the message.

Liability to Elmo's Trademark Owner

In this part, in addition to doing a solid prima facie analysis, I wanted your analysis to reflect Hornblower's multiple trademark uses—the website name ("Elmo Rehabilitator"), the domain name (elmorehabilitator.com), any references to Elmo on her website, and the encoded message in the bogus URL. In particular, I expected you to acknowledge the possible ACPA liability. If your answer didn't get granular about the different trademark activities or skipped the ACPA analysis, your score may have suffered.

Trademark Infringement

I assume the trademark owner has a valid trademark (note: "Elmo" is a personal name which, in the 1910s, was one of the 300 most popular boy's names according to NameVoyager) and has priority over Hornblower.

The use in commerce requirement could prove tricky. In my opinion, without more evidence of commercial behavior, this looks like an easy defense win. Her artistic endeavor is clear and undisputed, which should take her activity outside of trademark law.

However, the Lamparello "punt" shows that the analysis isn't so easy. First, some courts equate this factor with the Commerce clause analysis. Second, to the extent that she is "marketing" her non-commercial website, this could qualify as a use in commerce. Third, if the project is designed to help Hornblower build her own brand to increase awareness or sales of her other art projects, a court might deem the indirect brand-building commercial.

The likelihood of consumer confusion analysis is also irresolute. A lot depends on the actual content and appearance of elmorehabilitator.com. If it looks anything like the example I linked to, any visitor would instantly conclude that the project is independent from the trademark owner. Thus, even if visitors experienced some form of initial interest confusion (whatever that means) prompting them to look at the website, per Lamparello, there would not be any actionable confusion. However, the website could superficially look like an officially sanctioned effort to spread Elmo's love throughout the world. Certainly, trademark owners have done crazier things in the name of stimulating user engagement with their brands (Subservient Chicken comes to mind). Furthermore, target website operators might experience some "confusion" about why their server logs are being spammed, and they might (rightly or wrongly) assume the Elmo trademark owner is responsible.

Even if the prima facie infringement case is established, Hornblower could argue that her Elmo activities qualify as nominative use because they accurately refer to Elmo. There aren't many other good synonyms to describe "Elmo," and Hornblower would argue that she took only as much as necessary. (But, a court wonder if she needed to use Elmo in the domain name). As indicated in the previous paragraph, the harder inquiry is whether visitors would assume an implied sponsorship or endorsement of Hornblower's project by the trademark owners. The inclusion of "Elmo" in the domain name might imply a more official connection.

Dilution

We can assume Elmo's fame and that Hornblower's use commenced after the mark was famous. The use in commerce factor remains indeterminate. It is not clear that there is a likelihood of dilution. Because the usage is referential, Hornblower is not creating a new definition of "Elmo." (But see Mattel v. MCA, which we didn't discuss in class, where the Ninth Circuit said the song "Barbie Girl" added a new definition to "Barbie"). Further, Hornblower is trying to rehabilitate Elmo's reputation, so arguably there is no tarnishment. At the same time, Elmo's trademark owner could argue that Hornblower harmed the mark's reputation by associating the mark with a DDOS campaign and by inserting the mark in server log spam.

Hornblower would try to invoke all three dilution defenses: fair use (specifically, nominative use); commentary (the artistic statement); and non-commercial use.

Domain Name Protection

As I've already indicated, the domain name is specially regulated and deserves its own analysis. An ACPA challenge would likely fail for lacking "bad faith intent to profit" because Hornblower had no clear intent to generate cash. The UDRP standard of "bad faith" is less clear, in part because the UDRP is so complainant-favorable. Personally, I think an artistic purpose should be enough to negate bad faith (or, alternatively, evidence a legitimate purpose), but the connection with a DDOS campaign and server log spamming could be enough for a panelist to determine that Hornblower acted in bad faith even without financial motivation.

QUESTION 2 (mean word count of 564 words)

This was a really easy question! I wanted you to address three points:

- claims by defrauded users are presumptively preempted by 47 USC 230
- Roommates.com may represent a 230 hole because Shrugged encouraged illegal behavior—which the opinion specifically referenced as an exclusion
- 230(e)(1) excludes federal criminal law from 230's coverage, so if the US government pursues Shrugged under criminal law, 230 won't apply.

Many of you got to these three points, sometimes more clearly than others. Therefore, my grading was based on two considerations. First, did you miss one or more of these points? Second, did your overall discussion convince me that you understood the statute? As a result, misstatements or fuzzy/incomplete articulation of correct points were detrimental to your score.

Let me build out the analysis a little bit more:

Liability to Defrauded Users

47 USC 230 presumptively protects Shrugged from any claims by defrauded users:

(1) The game easily qualifies as an interactive computer service.
(2) Would a claim by the defrauded user treat Shrugged as a publisher or speaker? As we discussed, courts have almost uniformly taken the position that any claim against a service provider based on third party content/actions treats the service provider as a publisher or speaker unless it fits into the statutory exclusions ([federal] IP, federal criminal law, ECPA).
(3) Is the claim based on information provided by another information content provider? Cap commits the fraud by layering his own communications on top of the site's tools. There is nothing to suggest that Shrugged contributed anything specific to Cap's fraud.

However, the Roommates.com case contains a variety of statements that could be adverse to Shrugged. The most obvious statement is "If you don't encourage illegal content, or design your website to require users to input illegal content, you will be immune." There is no evidence that Shrugged required users to input illegal content, but Shrugged did *encourage* illegal content. After all, the game encourages users to lie to each other and says "fraud is fun," so this appears to be the kind of activity that could drop a site out of 230 protection.

There are two possible limits to this analysis. Shrugged could argue that some tortious conduct might still be outside the site's encouragement of lying and fraudulent behavior. I'm thinking of tortious battery in football. A player can legitimately mug his/her football opponent during game play without committing a tort, but a roundhouse kick to the opponent's head is never OK. So Shrugged might argue that Cap's behavior was the equivalent of a roundhouse kick in football and therefore outside the game's scope.

Alternatively, Shrugged could argue that, due to the deceitful milieu, all players contemplated real-world fraud was within game play. This may be an assumption of risk argument instead of a 47 USC 230 analysis, but it may help understand whether Shrugged actually encouraged illegal behavior.

Personally, I would be surprised if courts, even post-Roommates.com, would treat Shrugged as responsible for Cap's fraud despite the user encouragements. Note that in the three cases applying Roommates.com since the en banc opinion, all of them have cited language in the Roommates.com opinion *in favor of defendants*. Similarly, Shrugged could point to other language in the opinion, such as the "neutral tools" reference, to avoid liability.

Liability to the Federal Government

Cap's behavior might violate federal criminal law in a variety of ways—wire fraud, banking regulations, securities regulation, tax evasion, etc. Should the federal government bring criminal charges against Shrugged for Cap's behavior, Shrugged cannot claim 47 USC 230 as a defense. This doesn't mean Shrugged will be criminally liable in the end.

About the Question

This question is based on Eve Online, a multi-player game that encourages deceitful play (a founder actually said "fraud is fun"). In 2006, a player using the alias "Dentara Rast" successfully ran a Ponzi scheme in Eve Online, netting about $80,000. See http://www.gamerswithjobs.com/node/26703 I was recently at a law professor conference where the Dentara Rast situation was discussed, and I pointed out that 47 USC 230 almost undoubtedly protected Eve Online from any user claims. I was immediately chastised by other professors (who are, not coincidentally, enthusiastic gamers) who thought I was wrong. So I wanted to see what you thought.