Internet Law
Spring 2020
Final Sample Answers

These are sample answers, not authoritative ones. As long as you supported your analysis appropriately, it was often possible to reach opposite conclusions and still get full credit. These answers are longer than the word limits on the exam. I wrote drafts of them that came in under, but then I read your answers and you identified so many more interesting issues that I felt compelled to address them in the sample answers.

Question 1: Venture Capitalists: What Do They Know? Do They Know Things?? Let's Find Out! (1,879 words)

Summary

Cabracadabra needs to make serious changes to its hiring policies but can continue operating if it does. Clentists is legally fine and can continue as is. Oxnard needs better security and good terms of service, but these are both feasible. And Hollywood Heist is an ethical nightmare with severe and unfixable legal problems.

Cabracadabra

I will assume that a policy of hiring only female drivers as employees would violate Massachusetts law and that the harassment from male passengers would establish an illegal hostile working environment if proven at trial. I will consider only whether Cabracadabra's asserted defenses are sufficient to defeat these claims.

First, Cabracadabra may have a good argument that its drivers are ***independent contractors***. It is similarly situated to Uber in *In re Uber Technologies Inc*. Its drivers provide their own vehicles and choose when and how long to work. I would need to know more about how Cabracadabra pays drivers and its policies about how drivers must perform their work to say for certain whether the NLRB's reasoning about Uber would also apply to Cabracadabra. This reasoning may not work in states such as California which have adopted a more stringent test for determining whether a worker is an independent contractor.

Second, Cabracadabra probably does not have a ***Section 230*** defense as to either the hiring policy or the working environment. If the drivers are employees, then the ride offers are made to drivers by Cabracadabra, not by riders, so they are not third-party content provided by "another information content provider." Even if the drivers are independent contractors, Cabracadabra itself controls the aspect of the content — the discrimination on the basis of sex — that makes it illegal, as Cabracadabra itself does not allow riders to request rides from male drivers. It is thus like Roommates.com (discussed in *Dirty World*) and Section 230 does not apply. And either way, there is a good argument that Cabracadabra is like Airbnb in *City and County of San Francisco* (discussed in *La Park La Brea*): the law here regulates economic activity directly, rather than speech on Cabracadabra's platform. As for the hostile-working-environment claim, Section 230 does not apply to any speech from passengers that takes place offline in drivers' cars. The claim does not attempt to hold Cabracadabra liable as an "interactive computer service" and the harassment is not information provided by an "information content provider." (To the extent that the harassment takes place through the app, I believe the answer here turns on whether the drivers are classified as employees or as independent contractors.)

Third, I do not believe that Cabracadabra's ***terms of service*** will be effective to defeat the lawsuits. They probably fail to create a binding contract. The text "Remember that your use of this app is governed by terms and conditions" does not require drivers to take any action specifically manifesting their agreement to the terms and conditions. In this respect, it is more ambiguous than the language in either *Meyer* or *Cullinane*, both of which stated that the user agreed Uber's terms by creating an account. In addition, because the splash screen disappears after five seconds, even a reasonably diligent user might not actually have notice of the terms.

Even if the terms are binding as a contract, Cabracadabra has not presented any evidence that the contract has terms that would preclude the drivers' lawsuit, such as an arbitration clause. And in any event, a contract between Cabracadabra and its drivers could not serve as a defense to a claim that Cabracadabra is violating state employment law by hiring only female drivers. Non-drivers are not parties to the contract, and neither is the state of Massachusetts, nor could a private contract displace anti-discrimination law.

To summarize, I do not believe that Cabracadabra's app-based structure will insulate it from legal responsibility. It will probably need to end its policy of hiring only female drivers if it wants to continue operating — but that change will also eliminate its most distinctive feature.

Clentists

This may not be a promising business model, but there is nothing legally problematic about it. Dentistry is a regulated profession, but Clentists's dentists will not actually be performing dentistry online. They will be providing information and as such their speech will be fully protected under the First Amendment. State attempts to prevent them from providing this information online might also violate the Dormant Commerce Clause, as it would have the effect of regulating the speech available in states which do not attempt to restrict speech about dentistry. Clentists probably cannot, however, raise a Section 230 defense, as it appears the clown dentists would be Clentists' own employees (as in the analysis for Cabracadabra).

All this said, although Clentists is legally safe, it runs the risk that YouTube might take down its videos, as YouTube's policies on harmful content are more restrictive than the First Amendment, especially where medical information is involved. Clentists should also post a prominent disclaimer at the start of each video warning that the procedures shown should only be carried out by qualified and properly licensed dentists who should exercise their own professional judgment.

Oxnard

If MeowMeowFuzzyface's post is accurate, then Oxnard's statement in its privacy policy that it "protect[s] [user] personal information with industry leading security" is false. Leaving data unencrypted is not "industry leading security." Thus, Oxnard has committed a "deceptive act[] or practice[]" in violation of the Federal Trade Commission Act, 15 U.S.C. § 45(a). I do not believe that the use of cloud storage by itself violates Oxnard's promise not to "sell or disclose your personal information to third parties," but Oxnard should revise its privacy policy to be more clear on this point.

The Federal Trade Commission is likely to bring a civil enforcement action, as in *In re Snapchat*. The FTC is also likely to be concerned that Oxnard failed to

respond when MeowMeowFuzzyface brought the security issue to its attention. I recommend searching Oxnard's email archives to try to determine when and how MeowMeowFuzzyface made contact. The good news is that the FTC is likely to insist only on a consent decree requiring a more honest privacy policy, better data security, and a comprehensive privacy program going forward. The California Attorney general may also take action under the California CPA, which could result in substantial fines. In addition, MeowMeowFuzzyface's post shows that Oxnard has suffered a data breach that triggers reporting obligations under state data breach notification laws and the GDPR. It should provide the required notices ASAP.

VincentAdultman's post does not directly implicate the privacy policy. It does, however, raise serious questions about privacy risks going forward. If users' spaghetti strainers can be remotely deactivated, there is a risk that they could be remotely modified (e.g., to act as surveillance devices). Oxnard needs to investigate immediately and make appropriate fixes; if it does not, the FTC might add this to the list of actionably bad security practices. There is also a a risk that the strainers might be modified to make them dangerous: for example, by misreporting the temperature of extremely hot spaghetti.

Taken together, these concerns also present a risk of consumer suits: for violation of the privacy policy, for defectively nonfunctional products, and possibly for defectively dangerous products. Oxnard needs to have in place a stringent set of terms of service to block such claims and route any consumer suits to arbitration. Fortunately, Oxnard can use the Internet-connected aspects of the strainers to impose such terms: consumers need to be forced to click to agree when they first set up their strainers. (This technique may not be enforceable against consumer who have already purchased and set up their strainers unless Oxnard is prepared to offer a refund to any consumers who reject the new terms.)

Oxnard may be able to sue MeowMeowFuzzyface under the CFAA, but it should not. It may be difficult to identify MeowMeowFuzzyface, who is clearly skilled in computer security and may have covered their tracks. And more importantly, bringing suit would be terrible publicity and would draw the attention of other grey- and black-hat hackers. It does not appear that Oxnard has any vi-

able causes of action against VincentAdultman. Any attempt to hold Hackin4-Dayz secondarily liable would be barred by Section 230.

In short, Oxnard has serious legal issues, but they are fixable.

Hollywood Heist

Hollywood Heist's users will be blatantly violating the law in numerous ways:

- Hacking into a celebrity's phone is a violation of the Computer Fraud and Abuse Act. A smartphone is a "protected computer" under the CFAA, the hackers do not have "authorization" from the celebrities, and they will be "obtain[ing] information" in violation of 18 U.S.C. § 1030(a)(2)(3).
- The hackers are probably not violating the Stored Communications Act by accessing celebrities phones themselves, because a user's phone is not an "electronic communications system." But if the hackers then log into social media accounts using the hacked phones and retrieve messages from cloud-based accounts, that might be an SCA violation. (It will also be an additional CFAA violation, because it will also be access without authorization to the social media services' computers.)
- The hackers are committing intrusion on seclusion when they hack into celebrities' phones and view private information there.
- If the hackers cause any damage to the phones — such as deleting data or changing passwords — they are committing trespass to chattels.
- If the hackers share any sensitive information with Hollwood Heist or anyone else, they will be committing the tort of publicity given to private life.
- If the hackers post pretending to be the celebrities on social media, that may be a violation of anti-impersonation statutes such as the New York one at issue in *Golb I* and *Golb II*.

Hollywood Heist itself is likely to be held liable for at least some of its users' activities. It induces its users to violate the CFAA, SCA, and identity theft statutes. Thus, it might be prosecuted along with them under principles of accomplice liability or conspiracy. It also induces its users to commit intrusion on seclusion and publicity given to private life, and so could be jointly liable along with them.

Hollywood Heist probably cannot use Section 230 as a defense. The CFAA, SCA, and intrusion on seclusion theories do not purport to treat it as a publisher or speaker of third-party content. There is a strong argument under *Dirty World* that sensitive information posted on Hollywood Heist by users is not truly third-party content because of Hollywood Heist's own role in causing the users to obtain and post it. (*Cf. Accusearch*, discussed in *Dirty World*.) And when users impersonate celebrities on *other* platforms, Hollywood Heist is not being held liable as a "provider or user of an interactive computer service."

Similarly, the First Amendment probably does not shield Hollywood Heist. The fact that it pays users to commit these torts and crimes means that it is not merely advocating illegal activity, but participating in it. And when users post illegally obtained celebrity material, Hollywood Heist is not an innocent recipient as in *Bartnicki*.

In short, everything about Hollywood Heist is illegal and terrible and PB Enterprises should not invest.

Question 2: A Very Famous TV Show (1,600 words)

Summary

Vim and Vigor should use takedown notices under Section 512(c) to remove uploaded episodes from major platforms. It should consider using a UDRP to obtain the `horsinaround.show` domain name and consider a copyright suit against Todd Chavez. Although PrincessCarolyn, Diane Nguyen, and others are infringing Vim and Vigor's copyrights, it should refrain from suing them at this time.

PrincessCarolyn

By recording episodes of *Horsin' Around* as they aired, PrincessCarolyn infringed the reproduction right. At the time, this was probably have been fair use as personal home taping. Although *Sony*'s fair use holding involved time-shifting and PrincessCarolyn retained a complete archive of the show, this would probably still be a personal fair use as she was not substituting for authorized copies in any market. (The VCR maker — possibly but probably not Sony itself — is shielded by *Sony* and is probably long out of the statute of limitations anyway.)

Similar reasoning applies to PrincessCarolyn's digitization. The digital versions were new copies that infringed the reproduction right. The fair use defense here is weaker, since PrincessCarolyn already had usable copies, so the digitization was at best entirely for her convenience. Cutting in her favor, however, the lack of any authorized videocassette, DVD, or digital version of *Horsin' Around* meant that there was no authorized version she could have purchased.

When PrincessCarolyn uploaded the digitized files to YouTube, she infringed the reproduction right (for the uploads), public performance right (for the views by others users), and public distribution right (when other users downloaded the files, presumably by using YouTube downloader utilities). Here, her fair use case is at its weakest, since she shared the works with strangers — in fact, potentially with every Internet user in the world. That takes the case out of the *Sony* rationale for private home uses and makes it look much more like *Napster*. There still was no authorized alternative, but Vim and Vigor's plans to bring out an authorized edition show that there was in fact a viable market all along. Vim

and Vigor could argue that the widespread presence of pirated versions meant there was less of a market for a legitimate one.

There is no point in suing PrincessCarolyn now; the horse is out of the barn and many others already have the digital versions she made. In addition, she is a loyal superfan, and suing her would result in terrible publicity. Vim and Vigor's efforts would be better directed toward getting the episodes removed from YouTube and other platforms.

There is also the issue of identifying who "PrincessCarolyn" is. This would require a subpoena to YouTube for her account information. The infringement case against her is strong enough that the subpoena should be granted, but there is a risk the trail will dead-end there if she turns out to be overseas or not otherwise traceable.

Diane Nguyen and other users

Downloading the files PrincessCarolyn uploaded to YouTube is a reproduction; uploading them to other video-sharing sites is a reproduction and a public distribution. These users' (including Nguyen's) uploads are unlikely to be fair uses for the same reasons that PrincessCarolyn's weren't: they are non-transformative uses, shared with the general public, of complete works, in a way that undermines a normal licensing market. Again, it doesn't make sense to sue these individual fans; Vim and Vigor should focus on having the videos taken down (see below).

Nguyen's attempted relicensing of the videos under a Creative Commons license is ineffective. Nguyen is not the copyright owner; she has no authority to allow others to violate the copyright owner's exclusive rights. Thus, even though the license purports to allow others to copy the videos freely, those who do so are still infringers. That said, the fact that these videos are floating around on Vimeo with the license attached may be misleading others users into thinking sharing is allowed. This is a further reason not to sue individual users and also a further reason to have the videos taken down.

horsinaround.show

For the reasons already discussed, the individual users who upload *Horsin' Around* videos to `horsinaround.show` ("the Dot-Show Site") infringe and do not have good license or fair use defenses. (Individual downloaders also probably

also infringe for similar reasons, although in their case the private-use arguments cut slightly more in favor of fair use.) The bigger question is whether the Dot-Show Site itself infringes. Under the logic of *Giganews*, individual uploaders and downloaders are the direct infringers, not the Dot-Show Site. A counterargument is that the design of the Dot-Show Site is so focused on *Horsin' Around* episodes (including upload and search forms keyed to the list of episodes) that it in fact has the necessary volition. I believe, however, that these same considerations show why the site is secondarily liable, so the point may be moot.

The Dot-Show Site does not appear to be a vicarious infringer since there is no sign that it has any financial interest at all in the uploads. Perhaps more facts could be established to show that it does, such as future business plans as in *Napster*. It does, however, have the right and ability to control the infringing activity: it could turn off the episode-specific aspects of the forms and stop optimizing its design for infringing uploads.

The Dot-Show Site appears to be a contributory infringer. Its design shows that it has knowledge of the specific content users will be uploading: *Horsin' Around* episodes. To be sure, it does not know for certain *ex ante* that any particular upload will actually be a particular episode. But the design is so targeted that it is fair to attribute that knowledge to it. Similarly, the episode-specific design — together with the fact that it hosts the uploads at all — is a material contribution to the infringement. It does not have a *Sony* defense because it is a service and not a device and because it has specific knowledge of the uploaded works and their likely infringing nature.

The Dot-Show Site also appears to be an inducing infringer. The site design affirmatively encourages users to upload specific *Horsin' Around* episodes; the design itself is the "clear expression" of intent to induce infringement. Indeed, the site's very name helps indicate an intent to induce infringement. The material contribution analysis is the same as for contributory infringement.

The disclaimer on the Dot-Show Site is ineffective. Merely that the site is not responsible for user infringements does not relieve it of its obligations under copyright law.

There are not likely to be difficult jurisdictional issues in suing the Dot-Show Site. Although the servers are nominally in Poland, there will still be subject-matter jurisdiction over the case since there are downloads in the United

States. *See TV Polska*. And personal jurisdiction over Bojack/Todd Chavez will be proper in the Southern District of California, where he is domiciled. There is a possibility that Bojack is not in fact Todd Chavez; discovery will be necessary to determine whether this is the case. If Bojack is in fact in Poland, while it might be possible to get personal jurisdiction on the basis of providing infringing downloads in the United States, it may not be worth the effort given the difficulty of enforcing any judgment. I recommend starting by sending a cease-and-desist letter to Chavez.

Another option is to bring a UDRP to gain possession of the `horsinaround.show` domain name. The name is identical to the HORSIN AROUND trademark (I assume that there is one and that it is registered in the United States) and it does not appear that Bojack has any legitimate interests in the name. That said, it is not clear that a site that is merely infringing copyright is also infringing trademark law: the name accurately describes the contents. Still, I think the odds are good enough that a UDRP is worth bringing. I don't think the cost-benefit analysis works for a trademark or ACPA suit; the UDRP is worth pursuing simply because it is so fast, cheap, and low-risk.

DMCA Takedowns

To get the videos offline in advance of the release, the best move is to send a flurry of DMCA § 512(c) takedown notices. To start with, Vim and Vigor should send notices for any videos that appear or claim to be complete episodes or long (>5 minutes) clips. It is easy to form the necessary good-faith belief in infringement for these substantial copies; there are not likely to be any difficult fair use cases for these videos. There is no urgent commercial need to go after fan-made montages, compilations of their favorite short clips, supercuts, etc.

YouTube, Vimeo, and similar sites are likely to take down the videos as a matter of course. Most of the uploaders are unlikely to contest the notices; even if they do, our clear copyright ownership makes it easy for us to file the follow-up suits. We should also register the episodes as part of ContentID on YouTube, which will assist in keeping the files down.

The Dot-Show site is unlikely to honor takedown notices. This purportedly Polish site may not even have a registered DMCA agent. I believe that the site's *Horsin'Around*-specific design means that it has red flag knowledge of the in-

fringing uploads and is ineligible for the DMCA § 512(c) safe harbor. Still, we should send the notices: it will either get the episodes taken down or unambiguously take away the site's eligibility for the safe harbor.