Internet Law
Spring 2019
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.

Question 1: @HottestStartups (1,408 words)

Summary

EnforcerBot, Cryptid, Domain Roulette, and AnalogWhole present unacceptable legal risks and should not be funded. Sub-Ether-Net is also a pass: the theory of law that underlies its business model is false. Feelgood, M.D. is legally risky, but not a definitive "no." UDRPCheap is legally clear enough to proceed.

1. EnforcerBot

Sending automated notices is fine; they are legally effective. Additional DMCA takedown notices do not provide any additional legal advantage and may actively discourage websites from acting on them. Moreover, 30 minutes is probably not long enough to constitute "expeditious[]" removal; a longer waiting period is probably necessary.

I do not think that the notices themselves would open up EnforcerBot or its users to liability: there is no misrepresentation of any fact under § 512(f), just the repetition of true facts. Some of the targeted uses may be fair uses, and the failure to consider fair use is technically a § 512(f) violation under *Lenz*, but in practical terms courts have not awarded significant damages against those who send notices. Nor are the notices a CAN-SPAM violation or trespass to chattels, *see Hamidi*, and I do not think they trigger the predicates to CFAA liability — there is no "damage or loss." 18 U.S.C. § 1030(g).

My bigger concern is spamming text entry fields on websites. This could constitute "impairment to the integrity …of … a system," *id.* § 1030(e)(8). It is easy to imagine a website incurring costs of more than $5,000 to remove these comments. There might be questions about whether this conduct is "authorized" when a website has a text entry form for anyone to use, but the state of CFAA law is unsettled enough that I do not want to take that chance.

Conclusion: **no**, do not fund due to CFAA risk.

2. Cryptid

First, this is another CFAA problem. If these were traditional accounts on traditional banks' computers, password guessing to transfer the assets to one's own account would be access without authorization. The counter-argument here is that on a blockchain, all "access" to any participant's computer is allowed by that participant when they accept a block containing the proposed transaction. I think that the CFAA should not apply to this kind of private-key guessing; I am not certain a court would agree.

But even if Cryptid does not violate the CFAA, it is engaged in straightforward violation of state theft and property laws. Bitcoin and other cryptocurrencies are "property," just like domain names and accounts. *Kremen v. Cohen* would suggest that by password-guessing, Cryptid becomes liable for conversion.

*Conclusio*n: **no**, do not fund due to property-law violations.

3. Feelgood, M.D.

The first big risk here is the unlicensed practice of medicine. Feelgood can raise a Section 230 defense: it does not see patients or give medical advice, and any attempt to regulate it as such would be treating it as the speaker of the advice that doctors give through its app. This is a powerful argument in theory: Zoom is not engaged in the practice of medicine, even if some doctors see patience via Zoom videoconference. But in practice, the states may successfully argue that Feelgood's commissions, although technically from doctors, mean that it is charging for medical services — and that billing is not "information" protected by Section 230. This risk is inherent in the business model.

Feelgood also has substantial privacy issues, but these can probably be dealt with. It holds large amounts of sensitive medical information on users, which it shares with the doctors on the platform. All of this can be done appropriately and legally with user consent. But because health data is separately regulated (by HIPAA), I will need to do a more detailed review of how Feelgood stores and protects user data, when it discloses it, and how all of this is described to users.

Conclusion: **maybe**, due to uncertainty in Section 230 caselaw and with appropriate privacy policy.

4. Domain Roulette

Many of the domains Domain Roulette registers are likely to contain trademarked terms. Some of these trademark owners may be upset. Because Domain Roulette is just showing ads, and its entire business is predicated on the domains being just random combinations of words, it will have "no rights or legitimate interests in respect of the domain name," UDRP § 4.a.iii. Some trademark owners might persuasively argue that the domain names are also being used in bad faith to draw in users looking for the trademark owner's goods (even if no trademark is specifically targeted). And the large-scale nature of the venture is not a good fact. That said, Domain Roulette may be able to minimize this risk simply by immediately transferring the relevant domain to any trademark owner who complains.

Domain Roulette has a more serious problem with hijacking its users' browsers. Preventing them from closing their browser windows might constitute "damage" under the CFAA and it is hard to argue that this is a form of access that users "authorize." There will be no good way to make users agree to Domain Roulette's terms of service, since this would need to happen before hijacking their browsers, and they are not likely to click through a sign-up process on a random website they went to by accident. The Federal Trade Commission might also regard the hijacking as an unfair trade practice.

Conclusion: **no**, do not fund due to the risk of CFAA prosecution, user lawsuits, and FTC action.

5. Sub-Ether-Net

HavenCo also failed because potential customers were still subject to the regulatory jurisdiction of their own countries. Sub-Ether-Net is not going to be able to solve that problem for its customers. Saying, "Sorry, the data is on a submarine" is not going to be any more persuasive than saying, "Sorry, the data is in Ireland," which is not a valid excuse for subpoena compliance following the CLOUD Act. Any liability-creating content stored by Sub-Ether-Net will still be liability-creating. Also, this is just a terrible idea: submarines are expensive and vulnerable and the data will go offline whenever the submarine is submerged.

Conclusion: **no**, the legal advantages Sub-Ether-Net promises its customers do not actually exist.

6. UDRPCheap

This is … actually … a good idea? If their technology works and the financials of their business plan check out, fund them. UDRP proceedings are entirely online, so they are a good fit for purely digital filings. There is also a large dataset of previous UDRP outcomes so it is plausible that UDRPCheap could actually make good predictions. I will think about unauthorized-practice-of-law issues, but I am initially optimistic, as UDRPs are not tied to any specific legal system.

Conclusion: **yes**, this may be workable

7. AnalogWhole

I will want to do an audit of the open-source software that AnalogWhole is using, so that I can check for compliance with the licensing terms. I expect, however, that any violations can be cured either by using different open-source libraries, by writing necessary code, or by releasing AnalogWhole's additions under an appropriate license.

My bigger concern is copyright infringement. Some of the users who record programs using AnalogWhole will likely infringe (e.g. by sharing the recordings with strangers online). Others may make fair uses, but for programs recorded off of on-demand streaming services, the time-shifting argument is much weaker — you can always get the program at a time of your choosing from the streaming service, so you have no need to record it for that convenience. So some users will directly infringe, and there is a serious risk that AnalogWhole will be liable as an inducer. The device inarguably makes a material contribution to user infringements (as does the immediate upload to a cloud service), and it is so specifically designed to exfiltrate programs from the streaming services that a court might see AnalogWhole's marketing of it as an attempt to induce users to use it to infringe.

The good news, I suppose, is that the device is not likely to violate § 1201(a), because a user who uses it does not actually disable or bypass DRM to gain access to a copyrighted work. She merely copies the work once she has authorized access. But I think the copyright-infringement argument is bad enough for AnalogWhole that this is cold comfort.

Conclusion: **no**, do not fund due to copyright risk.

Question 2: Startup Sings the Blues (1,375 words)

Summary

First, I need to finish reading the terms and conditions. I will ask Trust and Safety to keep BlandSal suspended while they investigate his claim of being framed. I will ask Engineering to remove Fiona Gormlaith's content and to temporarily geoblock the affected recordings in Germany. I will send an email to the Alabama OAG declining to comply with their requests, and negotiate the "enhanced content location fee" with Bluegrass Broadband. And I will retain local counsel in Germany to research the underlying suit and tell us our options.

Terms and Conditions

The link in the footer is a good idea but not sufficient to make the terms binding on users. Presenting the terms and conditions *after* the user completes the signup process may mean that they are not binding even as to registered users. Users are on notice of the terms, but they have not been required to take action to indicate their agreement to the terms. It would be better to have an explicit checkbox as part of the signup process, so that users could not create an account unless they affirmatively indicated their agreement. The underline is a good choice in light of the *Uber* cases.

The substantive terms look good at first glance, but I will need to review them in more detail. Knowing exactly what the terms say is so important that I *must* make time to do it as soon as possible, regardless of what other pressing matters end up on my desk.

German Court Order

If this suit had been properly defended, Backroads would have had a reasonable case. As seen in the GDPR, even though European legal systems do not have the First Amendment, they still take historical concerns into account when assessing restrictions on the freedom of expression. So one option is to hire local counsel and immediately seek to reopen the case. I don't know enough about the German legal system to know the viability of this option, but I can probably find someone who does and get their quick opinion — certainly for less than EUR 50,000 per day.

A second option is to comply, or at least comply temporarily while we figure out whether we can reopen the case. I will ask Engineering whether geoblockking certain recordings in Germany is feasible. If we have a choice, I would rather block these specific recordings there. My second choice would be to temporarily geoblock all of Backroads for users in Germany, and my third choice would be to remove those recordings worldwide. 46 users in one country is not enough to justify taking down content that is of core interest to our worldwide user base. I will also need to reed the order more closely to determine how specifically it identifies the recordings at issue: I am more inclined to comply if it is a small number of specified recordings, and much less inclined to comply if it is all of our 1920s and 1930s recordings.

A third option, which I am less inclined to pursue, would be to ignore the order. Backroads is U.S.-based for now, and we would have a strong defense under the SPEECH Act for any attempt to enforce the German judgment here. But I do not want to get into a position where there are massive accrued fines in Germany against Backroads: it would put us at severe risk if we ever tried to expand more in Europe.

BlandSal

First, I will ask Trust and Safety to investigate BlandSal's claim that he was "framed" when he made posts impersonating another user. I have no idea how that could even happen, but Trust and Safety can get to the bottom of this. If he really was framed, we will reinstate the account for now and take appropriate action against BlindSal. But for now, I'll assume his claim is meritless.

If the terms of service were effective, they would completely block BlandSal's claims against Backroads. He has violated the policies on posting infringing and harassing content. Backroads can remove any content in its sole discretion. The liability waiver protects Backroads, and the case would go to arbitration in any event. Unfortunately, as noted above, they may not be binding.

BlandSal's claims are substantively weak. There is no copyright infringement liability for deleting a copy, the copies on Backroads until the ban were posted with BlandSal's permission, and it is a little unlikely that BlandSal is the copyright owner of old blues recordings in any event. The conversion argument might make some sense under *Kremen*, but it is difficult to extend *Kremen* to loss

of data rather than taking away some resource that only one person can hold, like a domain name or an account. (Why didn't he keep his own copy?) Backroads is not a state actor, so it is not restricted by the First Amendment. And there is absolutely nothing to suggest that Backroads has market power in any relevant market, or that it has made any agreements in restraint of trade.

Backroads's best defense, however, is Section 230. As an initial matter, BlindSal would have had no claim against Backroads had it taken no action against BlandSal: the impersonating posts were "information" posted by "another information content provider" and any lawsuit would have treated Backroads as the "publisher or speaker." Section 230(c)(2)(A) protects Backroads from liability for voluntarily restricting access to content Backroads considered objectionable, which the impersonating posts were. BlandSal could try to argue, as the plaintiffs in such cases always do, that the removal was not undertaken in "good faith." But the paper trail here is good: BlandSal has a history of unambiguously illegal and harmful posts. The only downside is that 230(c)(2) litigation can be slow and expensive due to the good-faith issue. Still, I think Backroads needs to stand firm. Assuming that Trust and Safety finds nothing to his claims of being framed, the account suspension should stand. We don't want him as a user.

Fiona Gormlaith

Gormlaith, as a user within the EU, probably has a right under GDPR art. 17 to have her personal data removed on the basis of withdrawal of consent. I will ask Engineering to investigate and carry out the removal. If there are any technical obstacles, I will deal with them as they arise, but assuming there are none, Backroads should comply.

Alabama Blues Legacy Act

As applied to Backroads, the Alabama BLA is preempted by Section 230(c)(1). The BLA attempts to hold Backroads, an interactive computer service, liable as the publisher of information (the post) provided by another information content provider (CrossroadsChris). *Hassell v. Bird* indicates that orders to remove content, and not just tort liability, are also preempted. I will email the Alabama OAG directing their attention to Section 230. The BLA is also likely in violation of the First Amendment, since it it is a viewpoint-based restriction on speech that causes no significant harm to any living person.

As for the demand for the identifying information of CrossroadsChris, I would prefer to take users' side as far as possible. Under the Stored Communications Act, Backroads, as a provider of an electronic communications service, may not voluntarily disclose "a record or other information pertaining to a subscriber to or customer … to any governmental entity," including the Alabama OAG. 18 U.S.C. § 2702(a)(3). I will direct the OAG's attention to § 2703(c), which describes the legal channels by which a governmental entity can obtain customer records. I anticipate receiving a subpoena or court order in the near future, which I will forward to CrossroadsChris so that they can contest it if they so desire.

Bluegrass Broadband

Because the FCC network neutrality regulations have been withdrawn, no law currently prohibits Bluegrass's shakedown tactics. I will ask the business operations and accounting departments to determine how much in revenue we currently make from users served by Bluegrass, and how much we reasonably could make with projected growth. If that number is substantially more than $1,000/month, we will pay it; if not, we won't. Either way, once I have the number in hand, I will call back the Bluegrass Content Partnership Division to negotiate down the "fee."