Santa Clara University

Internet Law (Law 793)
Final Exam Sample Answer
Prof. Eric Goldman • Fall 2019

Overall, this was an easy exam. We had done so many similar examples in class, and question 2 overlapped a lot with the midterm. Most of you got most of the big points—and everyone discussed Section 230 and 512, so Gandalf was pleased!

Question 1

This question is based on U.S. v. Bondarenko, 2019 WL 2450923 (D. Nev. June 12, 2019). Yes, an organization called Infraud really had the motto "In Fraud We Trust." No, it did not end well for the participants.

Does Boris Qualify for Section 230?

Note: I treat Boris like a sole proprietor of Infraud, i.e., his liability is coextensive with "Infraud's" liability.

Overall, Section 230 should protect Boris for many third-party content and actions on Infraud. Like all websites, Infraud qualifies as a provider of interactive computer services. Thus, Section 230 presumptively protects Boris for all claims based on third-party information. Boris will be liable for the content or activities of Jane, Karen, or Lois only when the claim fits into one of Section 230's statutory or common law exceptions.

Common Law Exceptions to Section 230—Roommates.com.

Infraud may match the Roommates.com majority's standard that "If you don't encourage illegal content, or design your website to require users to input illegal content, you will be immune." Infraud arguably encourages illegal content; as indicated by its motto, that is its raison d'être. Boris can counterargue that Infraud encouraged a mix of legal and illegal content, as illustrated by the small (<10%) amount of legal content on the site. This legitimate content might be sufficient evidence that Boris did not encourage *only* illegal content. Still, the site's architecture and overwhelming percentage of illegal content could persuade a judge to disqualify Section 230 protection. The Roommates.com common law exception has been fading in courts, but perhaps this would be a rare case where it applies.

Common Law Exceptions to Section 230—Online Marketplace Transactions

Infraud takes a cut of every transaction, including illegal ones. In light of the Airbnb and Amazon rulings, Section 230 may not apply to transaction processing. We have not seen other marketplaces, like eBay, lose Section 230 protection (yet?). This evolving jurisprudence makes it hard to predict if this common law exception would apply to Infraud.

Common Law Exceptions to Section 230—Civil Conspiracy

We didn't discuss civil conspiracy in class, but Boris may be in cahoots with other criminal actors, so a civil conspiracy claim for their actions might work around Section 230.

Common Law Exceptions to Section 230—Liability for Moderators/Super-Users

The site designates "administrators" with extra powers over other users' content. While the administrators probably don't qualify as agents, their powers nevertheless could cause a court to treat them as first-parties of the Infraud enterprise rather than as independent third parties. If so, Boris may not have immunity for Karen's actions, at least within the scope of her authority. However, due to her site-wide powers, I think the common law exception (if it applies at all) would apply to all of her on-site actions.

Statutory Exceptions

We don't have any evidence to support the ECPA and FOSTA exceptions. However, the IP and federal crimes exceptions are in play, as discussed below.

Sub-conclusion on Section 230

Section 230 is a powerful defense, so it should protect Boris from a wide range of claims. However, the facts create several gray areas where Section 230 may not apply. Accordingly, it would be appropriate to analyze Boris' liability with and without Section 230 protection.

Liability for Jane

Prima Facie Case Against Jane—Copyright Infringement

Section 230 does not apply to federal copyright claims.

Jane commits direct copyright infringement by distributing third-party copyrighted works. It's unclear if she delivers copies to buyers electronically or in hard copy. If the former, Jane also reproduces the work. We don't have evidence that the copyrights are registered, though registration is typical for major copyrighted works like Hollywood movies. Thus, the copyright owners probably have standing to sue, and they will be eligible for statutory damages and attorneys' fees if their registrations are timely.

Jane's fair use defense is not compelling:

- She profits from selling the works.
- Selling unpublished footage is extremely unlikely to qualify as fair use (Harper & Row). Also, movies are often fictional, which is less likely to qualify as fair use.
- The facts don't indicate if she sold all of the films' footage or only segments. The latter might move this factor more towards fair use, but not if the segments are the "heart" of

the work. Courts can tautologically reach that determination by citing the buyers' interest in the offerings.
- Selling commercialized movies can displace the copyright owner's revenues, even if piracy sometimes acts as marketing for the movies.

Jane is most likely a direct copyright infringer.

Boris' Secondary Liability for Jane's Infringement

Contributory infringement. Like Veoh, Boris generally "knows" that infringing works are being vended on the site. The "Infraud" brand further inculpates Boris. However, we don't have evidence that Boris knew of any specific acts of infringement. We'd need to see if such evidence turns up in discovery (if a plaintiff gets that far).

Separately, Boris' shift of power to administrators could be considered willful blindness, as he has set up an enterprise filled with infringing activity and yet personally turned a blind eye to the consequences.

If Boris has the requisite knowledge, then his failure to terminate "known" infringing listings will constitute contributory infringement.

Vicarious infringement. Boris as site operator has the technical capacity to supervise the infringing acts. Many of you argued this on your exams but didn't acknowledge that this is true for every website. By delegating responsibility for site issues to administrators, Boris could claim that they, not he, possess the requisite supervisory capacity. Boris could also argue that he lacked any direct financial interest in the infringements because his cut wasn't specific to infringing items; he took the same amount for infringing items as he did for legitimate items. Still, the fact that such a high percentage of site activity is illegitimate will weigh against Boris. Just like how the Supreme Court couldn't ignore that 90% of Grokster's activity may have been infringing, a court won't sympathize with Infraud's heavy illegality.

Inducement. As we discussed in class, inducement claims rarely succeed, especially when contributory or vicarious infringement claims fail. Still, the facts suggest inducement. The legal standard is providing a service "with the object of promoting its use to infringe copyright." Infraud did not explicitly do that; it promoted illegality of all kinds, not just copyright infringement. I doubt a court would find that distinction persuasive.

Fair use. Boris' fair use defense isn't likely. The analysis looks similar to Jane's, except that Boris only takes a 5% cut instead of Jane getting 95% of revenues. Because Boris still profits from infringement, just less, I think the conclusion would be the same.

Section 512 Defense

Boris can assert a 512(c) defense for Jane's infringing activity. Some of the key points:

- stored at the user's direction. If Infraud hosts Jane's infringing content, then those materials are stored at her direction. Otherwise, Infraud only hosts promotions for the infringing items, not the infringing items themselves. In that case, Infraud could claim 512(c) for the promotions but possibly not the underlying transactions.
- Reasonably implement a repeat infringer policy. Copyright owners might question if Boris' repeat infringer policy is reasonable. We don't have specific evidence on this point, but we do know that Infraud has a persistent category of "Stolen Movies" with repeat sellers.
- Boris' knowledge/red flags. In theory, Boris might not "know" of any infringing acts until he receives 512(c)(3) notices. The facts don't specify Boris ever receiving 512(c)(3) notices, so Boris may lack disqualifying scienter. Further, simply having a category called "Stolen Movies" isn't enough (see Perfect 10 v. ccBill). Having said that, the combination of a category called "Stolen Movies," plus the availability of pre-release blockbuster movies for sale, makes it implausible that Boris didn't know or have red flags of widespread infringing activities. That makes the case similar to isoHunt. If Boris has the requisite knowledge of infringement, his failure to act expeditiously would disqualify 512(c).
- Right/ability to control. Per Veoh, "control" only applies to specific known acts of infringement, not generally. In this case, it likely means that Boris must intervene when he has the requisite knowledge (though that seemingly collapses this factor into the prior one).
- Direct financial interest in the infringement. Arguably, Boris' share of the infringing revenue would disqualify 512(c). However, perhaps Veoh means that disqualification only occurs with *known* specific acts of infringement, which (as discussed above) we're not sure Boris ever had.
- Inducement/willful blindness. If a court concludes that Boris induced infringement or had willful blindness, it might conclude that 512(c) is categorically unavailable.

Criminal Copyright Infringement

Jane is likely committing criminal copyright infringement. She infringes for commercial advantage, the work involves $1K or more of a value, and some of the works are prerelease (any one of these would suffice). We don't have the facts to determine her willfulness, but it doesn't look good for her. Boris may be equally exposed if the government can show his willfulness. Boris didn't "intend" to infringe any particular item sold by Jane or other users, but all of the scienter discussion above—including willful blindness and the "stolen movies" category—could be cited against him. Alternatively, prosecutors could claim he's Jane's co-conspirator.

Liability for Trade Secret Misappropriation

Jane misappropriates trade secrets. With respect to Boris' liability, Section 230 would apply to a Defend Trade Secret Act claim as well as state trade secret claims in Ninth Circuit courts. In other circumstances, Section 230 would not apply and other rules would—maybe a notice-and-takedown scheme?

Liability for Karen

Liability for Stolen Credit Cards

The facts state that Karen sells stolen credit card numbers and that intentionally selling such numbers violates state and federal crimes.

With respect to Boris' liability for Karen's illegal conduct, Boris can invoke Section 230 for the state crimes. However, due to Karen's administrator status, state prosecutors could argue that Boris and Karen are engaged in a criminal conspiracy or that Boris is an accomplice or aider/abettor.

Section 230 is categorically unavailable for federal criminal prosecutions. Thus, Boris could be liable if he has the requisite "intent," or if the conspiracy/accomplice/aider-abettor theories work.

Liability for Defamation

Karen called Victor a fraudster, which is probably an opinion. It's like name-calling and can't be proven/disproven. As a result, it's probably not actionable.

In contrast, the statement that Victor sold unusable credit card numbers is probably a factual claim because it can be proven/disproven. Karen communicated the claim to other readers. But does it injure Victor's reputation? Victor seeks to establish a reputation as a trustworthy seller of illegal items, and Karen claims Victor is an untrustworthy criminal. That degrades the willingness of buyers to transact with Victor, but the illegal transactions themselves damage Victor's reputation. Similarly, Victor could argue that Karen's claim is per se defamatory because it relates to his business dealings, but the court won't protect Victor's reputation for illegal dealings.

We don't have enough facts to evaluate if Karen's claim is true. Karen can also claim the First Amendment defense. Exposing the sale of illegal credit card numbers should qualify as a matter of public concern, but we don't have sympathy for buyers of fraudulent credit card numbers. If the matter is a public concern, Victor isn't likely to be a public figure generally, through perhaps he is a public figure in the Infraud community. If he is, Karen is liable only if she had malice. If Karen just made up the claim to stick it to her competitor, then she may have malice.

Section 230 nominally covers Boris for Karen's possible defamation. Victor could argue that Karen's status as an administrator disqualifies 230 in her case, especially because Karen's post gets heightened exposure due to her status. If Section 230 doesn't apply, Boris would be a republisher, and Boris would be equally liable with Karen if he received notice. We don't know if Victor notified Boris. If Boris qualifies as the original publisher, then strict liability would apply (subject to the possible First Amendment defense).

Liability for Lois

Trademark Liability

Lois references the "Goop" trademark in its domain name, which is displayed in the ad copy, and Lois' knockoff versions may be counterfeits or otherwise infringing.

The trademark registration provides prima facie evidence of Goop's validity. The trademark owner has priority (Lois is invoking it). Lois uses the trademark in the ad copy, which is a use in commerce. However, does Lois' usage create a likelihood of consumer confusion? The phrase "fakegoop" clearly signals distance from the trademark owner and acts as a warning to buyers. Consumer confusion isn't really plausible. Lois could also claim the nominative use defense because "fake Goop" refers to the original Goop. There's no other way to make the reference efficiently, Lois only took the name and not the other Goop brand elements, and the name rebuts any implied sponsorship or endorsement.

Nevertheless, Lois' activity probably is not OK, especially when associated with the knockoffs. For example, a variety of doctrines we didn't cover in class, such as post-sale confusion, suppress knockoffs. Also, knockoffs can create trademark problems under trade dress or other trademark doctrines—and if they are counterfeits, they create criminal exposure. Lois' references might also create false advertising problems.

Goop may have a dilution claim if its trademark is widely recognized by the general public. It might be given its notoriety; I'd like to see consumer surveys. Goop would claim that Lois' fakes create blurring, forcing consumers to wonder if they are getting the real or fake version, and might constitute tarnishment if the fakes sullied the trademark's reputation. Lois' nominative defense might apply. Even if Lois committed dilution, Boris likely wouldn't be liable for it because of the lack of contributory/vicarious dilution doctrines.

Boris may face liability for contributory trademark infringement for running Lois' ads. Federal trademark claims fit into Section 230's IP exception. The knockoff goods are sold off-Infraud, so Boris does not control the associated "instrumentalities." Same with the domain name itself. However, if the ad itself constitutes trademark infringement, then Boris might be in control if his service hosts the ads. Still, Goop would need to show that Boris "knew" of the infringement, and we don't have the facts to evaluate that.

Boris could invoke the 1114(2) "innocent infringer" defense as the "innocent" publisher of third-party ads. This defense rarely succeeds, and it's mind-boggling to think that a service with the motto "In Fraud We Trust" could be declared "innocent" of any user misbehavior.

Publicity Rights Liability

Lois' ad displayed Gwyneth's face and her first name. A single first name isn't always identifiable, but here it's combined with the face and thus identifies Gwyneth. The devil-horn modifications do not obscure Gwyneth's face, but they do support an unlikely-to-succeed parody

defense. In the end, Lois used Gwyneth's face and name in ad copy—a prima facie publicity rights violation.

Boris can claim Section 230 immunity for Lois' publicity rights violation depending on venue. In the Ninth Circuit, per *ccBill*, Section 230 applies to state publicity rights claims. Elsewhere, publicity rights claims are part of the IP exclusion to Section 230. If Section 230 does not apply to Boris' liability for Lois' publicity rights violation, then we aren't sure what the rule would be; possibly notice-and-takedown.

Question 2

This question is based on DHI Group, Inc. v. Kent, 2017 WL 4837730 (S.D. Tex. Oct. 26, 2017). Sadly, Oilpro did not survive much longer, but its competitor RigZone is still around.

Breach of Contract

Contract Formation

Rigged's employee created a registered Oilpro account. The account creation page displays the language: "By joining, you agree to our terms and conditions and privacy policy," where the words "terms and conditions" and "privacy policy" are bolded and link to the associated documents.

Superficially, this looks like a mandatory non-leaky clickthrough agreement. All registered users pass through this screen, and the site displays an if/then statement purporting to bind users to the terms. Presumptively, this is a binding contract.

However, there are problems with Oilpro's clickthrough presentation, including:

- The if/then statement. The button says "create your account." The if/then statement says "by joining." This verb mismatch isn't necessarily fatal, but it adds avoidable confusion.
- Font size/color. The call-to-action font size is the smallest on the screenshot; and it's visually overshadowed by the command to "create your account," which encourages users to act without further scrutiny. More crucially, it's easy to miss the white font on a light background. A user rushing to create the account might reasonably overlook the small white-on-light text.
- Hyperlink presentation. In Meyer v. Uber, hyperlinks were blue and underlined. Here, the hyperlinks are just bolded. Would a reasonably prudent user recognize this hyperlink? Possibly, but the Meyer v. Uber facts don't validate this approach.
- Call-to-action placement. The call-to-action is near the "create your account" button, which tends to support formation, but it's below the button. Thus, the call-to-action could be cut off in some screen displays, and those users would not be on notice of the terms.

Oilpro's formation process is suboptimal, but many courts would uphold it. Those that don't might embrace the Berkson v. GoGo "sign-in-wrap" standard, which requires a second click to form the T&Cs, which Oilpro did not do.

While I think the contract was properly formed, let's consider two alternatives.

First, the T&Cs purport to bind users who "visit" Oilpro. Because users wouldn't see this provision unless they visit the T&Cs page, this language is almost certainly not binding.

Second, citing Register.com v. Verio, Oilpro could say that Rigged took the contract benefits knowing the applicable terms. Verio conceded it knew of the terms, but Rigged may not make that concession. If the registration process didn't confer sufficient knowledge of the contract terms, then Rigged may not have obtained knowledge elsewhere. In contrast, Register.com sent a C&D to Verio communicating the contract terms; and Verio got reminded of the terms with every search. Neither happened in Rigged's case. Nevertheless, Rigged runs a rival site to Oilpro, so odds are good that it reviewed Oilpro as part of routine competitor monitoring, plus Rigged probably understood that Oilpro didn't want it to scrape. I think Meyer v. Uber is a better path to contract formation, but Register.com v. Verio could also apply if Oilpro can find sufficient evidence of Rigged's knowledge of the terms.

Amendment. The T&Cs say that usage of the site automatically accepts any updated terms, even if no other notice is provided. I think this runs afoul of Blockbuster, which jeopardizes amendable-without-notice contracts as illusory.

Contract Breach. The facts specify that the T&Cs ban script usage and email address collection, both of which Rigged breached.

Trespass to Chattels Doctrines

System Use. Rigged uses Oilpro's system when it deployed the automated script to gather email addresses.

Lack of Authorization. Oilpro tried to restrict authorization in several ways:

- The T&Cs expressly ban script usage and email address collection. If Rigged agreed to the T&Cs, then it had knowledge of these provisions. Or, Rigged may have constructive knowledge of the provisions despite lack of contract formation. However, per Nosal, T&Cs can't delimit server usage for CFAA purposes.
- The robots.txt file restricted automated site access. We don't have any evidence Rigged reviewed the robots.txt file, but was Rigged on constructive notice?
- The rate-limiting software. Rigged never exceeded the software's threshold, so Rigged probably never knew of its existence.

Without evidence of a C&D, Rigged's knowledge of Oilpro's restrictions is circumstantial. Still, as with Verio, it seems hard to believe that Rigged didn't know of the restrictions.

Common Law Trespass to Chattels

Under the CA rule, Oilpro has to show that Rigged caused, or threatened to cause, measurable loss to computer system resources. Rigged's activities didn't trigger the rate-limiting software, so its scraping didn't significantly affect Oilpro's servers. Furthermore, Rigged isn't likely to return soon, so it's not an immediate threat to cause future measurable losses.

Under the majority rule, Oilpro can show that it deployed self-help in the form of the robots.txt file and the rate-limiting software. However, robots.txt is not a technical block, and Rigged complied with the rate-limiting software. We don't have any evidence that Oilpro otherwise tried to stop Rigged's behavior, and if Rigged isn't coming back soon, it hasn't attempted to defeat those blocks.

Still, other companies would be very interested in harvesting email addresses from Oilpro. The cumulative effect of these scrapers could impact Oilpro's operations, even if Rigged did not.

Computer Fraud & Abuse Act

Nosal raises problems with Rigged's lack of authorization. Further, Rigged's activity apparently did not cause any damage that the CFAA recognizes. However, if Oilpro can show that it spent $5,000 on verification and corrective measures, then Oilpro has a case. Note: the hiQ v. LinkedIn Ninth Circuit ruling raises further doubts about the CFAA's applicability.

California Penal Code 502

If Rigged's use was unauthorized, then Oilpro's efforts to verify and correct Rigged's activities should satisfy 502.

CAN-SPAM

Oilpro lacks standing to sue Rigged for any unsolicited emails to Oilpro's users unless Oilpro acted as their email service provider.