



Internet Law (Law 793)
Final Exam Sample Answer
Prof. Eric Goldman • Spring 2023

Overview

I drew inspiration for this question from *United States v. Smith*, 22 F.4th 1236 (11th Cir. 2022).

Most student grouped their answers into five categories: breach of contract, trespass to chattels, copyright, trademark, and Section 230 (including defamation and the 230 exceptions).

CMF's Liability to SR (Other Than User Uploads)

Breach of Contract

Contract Formation. SR's implementation is a "clickwrap" because it requires two clicks, first on the checkbox to the left of the "I have read and agree to the website terms and conditions" line, and the second on the "place order" button. (It's not a "scrollwrap" because scrolling isn't mandatory). Two-click implementations like this have a very high likelihood of enforceability. However, SR's implementation is sub-optimal:

- The page is cluttered, and the call-to-action is harder to see due to the surrounding grey shading. On the plus side, the call-to-action is right above the "place order" button so that buyers can't miss it.
- The call-to-action doesn't use if/then grammar, though the user's check confirming agreement to the terms still expressly confirms assent.
- The call-to-action refers to the "website terms and conditions," but it links to a document called "end-user license agreement and terms of use." I think the cross-reference is still clear enough to buyers, but a textualist judge could throw out the assent due to the inaccurate call-to-action. Only about 10% of student exams noted this discrepancy.

Despite the call-to-action ambiguity, I think it's highly likely that a court would uphold SR's contract formation process. After completing the purchase, CMF should be bound to the terms.

The facts specify the formation process isn't leaky ("SecretReefs requires all purchasers to go through the following screens"). Some of you equated leakiness with obscure calls-to-action, but leakiness refers to alternative navigation options that bypass the intended formation process.

The robot exclusion headers cannot form a Meyers-style contract due to their lack of visibility and mechanism to manifest assent.

Register.com Workaround. Register.com may apply if a party takes contract benefits knowing the applicable terms. CMF apparently didn't know SR's terms before using the automated script. CMF didn't check the robot exclusion header and didn't see the T&Cs pre-checkout, after the

script already ran. I don't see any reason why CMF should be charged with constructive knowledge for either the REH or T&Cs (pre-checkout). CMF knows of the T&Cs post-checkout, so the T&Cs govern any future automated activity per Meyers formation principles (without relying on Register.com).

Contract Breach. The T&Cs "disallowed the use of any automated scripts to access its website." CMF's automated order placement using an automated process almost certainly breaches this provision. Ticketmaster v. RMG. However, because CMF wasn't bound by those terms at the time it used the automated process, it didn't breach the T&Cs. Many of you missed this latter point.

Trespass to Chattels

Chattel Usage. The chattel at issue is SR's servers, routers, and other equipment used to connect to the Internet. CMF used the chattel when it engaged with CMF's website to place its order.

Authorization. CMF used SR's chattel exactly for the purposes they were designed for. CMF acted like an ordinary customer, except for the speed by which CMF placed orders, which enabled an unusually large order size. SR tried to limit CMF's authorization to engage in this activity, including:

- The throttling software. However, the software never communicated the rate limit to CMF; it capped CMF's activity automatically.
- Robot exclusion headers. The REHs signaled that CMF's automated activity wasn't permitted, but CMF didn't see it, and no court has charged website users with constructive knowledge of REHs.
- The T&Cs. CMF learned of the terms after engaging in the restricted conduct, so the T&Cs did not remove CMF's implied authorization to use the site like other buyers. Van Buren also raised concerns about whether T&Cs can delimit authorization for CFAA purposes, but it didn't resolve that issue.

SR probably didn't withdraw CMF's authorization to use SR's chattel before CMF completed the automated activity.

Harm (CA Common Law TTC). SR's web servers suffered no apparent harm from the automated order-placing because the throttling software avoided potential problems. However, SR's system suffered a measurable loss when other orders were delayed. The loss should be de minimis because the brief delay probably had no further harmful consequences, but per Hamidi, it seems measurable. CMF might counterargue that SR never expressly delimited use of the email server, that CMF couldn't control how SR fulfilled the order, and that other emails sent to other customers also caused any delay. However, SR might be able to show that it prophylactically restricted automated activity to prevent bulk orders that would overload its email server. SR could also show the risks of third-party copycat activity, though perhaps only direct competitors would grab as much material as CMF grabbed.

Harm (CFAA). SR could count any remediation efforts towards the \$5k loss requirement, though it's not clear what remediation efforts are necessary or appropriate given that SR's chattels worked as designed. Otherwise, SR may not have suffered any recognizable CFAA loss.

Harm (502). Any remediation efforts would be SR's best bet to establishing this claim, but the facts didn't provide evidence of any harm that 502 recognizes.

Overall, SR's claims for the various trespass to chattels doctrines are weak. SR has a difficult time showing that CMF lacked authorization when it was placing orders consistent with SR's standard order-taking process; and the system harm was minimal.

Trademark Infringement

Prima Facie Elements.

- Ownership of valid trademark. The "SecretReefs" trademark is likely a descriptive trademark (like "Toys R Us," it describes the retailer's offerings). Mark registration indicates it achieved secondary meaning and is protectable.
- Priority. The facts specify that SecretReefs preceded CMF.
- Use in commerce. If the factor coincides Congress' Commerce Clause authority, both the keyword ads and keyword metatags constitute a use of SR's trademark in commerce. Under the definition restricted to ad copy and product packaging, the keyword ad copy would still clearly qualify. Network Automation specified keyword ad buys of trademarked terms constitutes a use in commerce. In contrast, keyword metatags aren't ordinarily visible to consumers, but courts have treated keyword metatags as commercial promotions nonetheless.
 - Some of you analyzed SR's usage for this factor. The first element (TM ownership) requires the plaintiff's use in commerce. This factor focuses on the *defendant's* use of the plaintiff's mark in commerce.
- Likelihood of consumer confusion.
 - Many courts have held that using the plaintiff's trademarks to trigger keyword ads, standing alone, does not create consumer confusion.
 - With respect to the keyword ad copy, Network Automation prioritized four factors:
 - Mark strength. Descriptive marks are sometimes weak, but "SecretReefs" has achieved recognition among fishers.
 - Actual confusion. No evidence on this point, but some courts use initial interest confusion as a substitute for incidents of actual confusion.
 - Purchaser care. Fishers carefully source navigation information given navigation hazards and to not waste time.
 - "Labeling and appearance of the advertisements and the surrounding context on the screen displaying the results page." Google labels its ads. Also, CMF's ad copy expressly discloses it as the source, which helps if consumers know that SR and CMF are independent.
 - Overall, the keyword ad copy probably doesn't create a likelihood of consumer confusion.

- The keyword metatags don't affect what information consumers see, so they have no risk of creating consumer confusion. Nevertheless, courts routinely treat the inclusion of third-party trademarks in keyword metatags as per se infringing.
- Per Network Automation, initial interest confusion should merge into the standard likelihood of consumer confusion analysis. Keyword metatags don't capture initial consumer attention (per Brookfield) because they don't capture any attention at all; and keyword ads should be evaluated in conjunction with the websites they promote (Lamparello).

A number of you were confused by the second Sleekcraft factor (“defendant’s use”). It assesses the litigants’ competitive proximity, which in this case is extremely high because CMF and SR compete directly.

Descriptive Fair Use Defense. I categorized SecretReefs as a descriptive mark (if you categorized SecretReefs as a suggestive mark, then descriptive fair use does not apply). CMF used the phrase “secret reefs” to describe not-well-known reef locations. This looks like descriptive fair use because CMF used the “trademark” terms for their dictionary meaning. This would excuse CMF’s usage of the phrase “secret reefs” in the keyword metatags and keyword ad copy. Promatek nominally supports this conclusion by saying trademarks can be used in keyword metatags when it’s a “legitimate” use, which I think includes descriptive fair use. (If you want to dig into this more, see the old Playboy v. Welles case). Only about 25% of you discussed descriptive fair use.

All told, whether due to the lack of consumer confusion or the descriptive fair use defense, I think CMF’s keyword ads and keyword metatags are not likely to infringe SR’s trademark.

Dilution. Ownership and priority were discussed above. SR is a niche website for the fishing community, so I don’t think it has recognition among the general consuming public in the US to qualify as a famous mark. It’s unclear if there’s any likelihood of dilution. CMF isn’t adding a new meaning to SR, nor is it associating SR with porn or making other unwanted associations. Furthermore, the dilution defense of “fair use” should apply. SR’s dilution claim has no chance of succeeding.

CMF’s Liability for User Uploads

User-Uploaded 3D Maps (Copyright)

Prima Facie Direct Infringement by Users for Uploading.

- Ownership of a valid copyright. Maps are copyrightable; SR’s maps convey the facts using lines, colors, and other expressive choices. SR fixed the maps when it created them electronically. SR’s copyright registration for its “website” might already include the maps published on the website at registration time. SR has likely cleared the preconditions for enforcing its map copyrights in court.
- Violation of 106 Rights. By uploading the maps, the users copy, distribute, and publicly display the works.

A number of you only discussed CMF's direct infringement, not infringement by its users, which meant you didn't show the predicate infringement for secondary infringement or analyze users' eligibility for fair use.

Users' Permission to Upload Maps.

Users likely have SR's permission to download maps, either expressly or implicitly. Does that permission extend to public uploads? We don't know what the T&Cs say about the maps (the T&Cs restrict uploads of proprietary GPS coordinates, but not necessarily maps).

A few of you discussed the first sale doctrine, which we didn't cover it in class. The first sale doctrine only applies to chattels and doesn't apply to digital files. (Also, it only excuses distributions, not reproductions).

Fair Use for Users' Uploads.

- Nature of use. Each user's upload isn't being done for profit, but it's not a "nonprofit educational" use either. The uploads are not transformative because they add nothing new. This factor favors SR.
- Nature of work. Maps are factual in nature. This factor favors CMF.
- Amount/substantiality of portion taken. Each user copies 100% of each map. This factor favors SR.
- Effect on the market. Maps on CMF may directly substitute for SR's offerings. This would reduce buyer willingness to pay for the paywalled bundle of proprietary GPS coordinates and maps. This factor favors SR.

Individual users' uploads are probably not fair use. SR has strong claims of direct copyright infringement against uploading users.

Prima Facie Direct Infringement by CMF. Per Cablevision, CMF can argue that it did not act volitionally when users uploaded their files to its system.

Prima Facie Contributory Infringement by CMF.

- Direct infringement. Uploading users are the direct infringers.
- Scierter. CMF encouraged uploads, but uploads are not always infringing. That depends on fair use, upload permissions in SR's T&Cs, and other defenses available to uploading users. So does CMF "know" of users' infringements?
- Material Contribution. Hosting known infringing files satisfies this requirement. SR could also argue that CMF "induces, causes or materially contributes" to users' infringements by encouraging the map uploads. If CMF should presume that map uploads are infringing, CMF may have "induced" infringement ("promotes its site to infringe copyright") by seeking users' infringing uploads.

SR has a good claim of contributory copyright infringement against CMF.

Prima Facie Vicarious Infringement by CMF.

- Direct infringement. Uploading users are the direct infringers.
- Right/Ability to Supervise Users' Acts. CMF could terminate users' account or remove their uploads, but this is true of every UGC service, so courts often look for something more. SR might argue that CMF's encouragement of illicit uploads casts CMF as the supervisor of users' actions.
- Direct financial interest. CMF is ad-supported, so its revenues nominally grow as users upload more infringing content. However, CMF's revenues also increase with legal uploads, so courts might discount the infringement-based revenue.

SR's vicarious copyright infringement claim against CMF is uncertain.

Section 512.

CMF can assert a 512(c) defense against direct, contributory, and vicarious infringement:

- Qualify as a "service provider." Websites are service providers.
- Material stored at user's direction. Users upload the maps.
- Adopt repeat infringer policy. Specified by the facts.
- Reasonably implement that policy. A five-strike policy nominally satisfies the DMCA's provisions, but some courts balk at generous strike counts. Courts may conclude that the service hasn't reasonably implemented a policy if it's never triggered.
- Communicate that policy to users. Specified by the facts.
- Accommodate "standard technical measures." Courts have not designated any technology as an STM.
- Designate an agent to receive §512(c)(3) notices. Specified by the facts.
- Post its agent's contact info on its website. Specified by the facts.
- No actual knowledge or red flags. Typically, actual knowledge comes from takedown notices, which CMF hasn't received yet. In the DMCA context, CMF's general knowledge that user uploads infringe doesn't constitute disqualifying scienter (Veoh). SR would nevertheless cite CMF's encouragement of users' uploads of maps, knowing that they are paywalled.
- No right/ability to control infringement. In the DMCA context, this applies to specific known instances of infringement, and only when the service exerts substantial influence over users. Without takedown notices, CMF may not know which specific instances are infringing. However, courts may decide that CMF's encouragement of presumptively infringing uploads might qualify as "substantial influence."
- No direct financial interest in infringement. For DMCA purposes, CMF probably doesn't have a direct financial interest because it doesn't profit specifically from infringing activity.
- Expediently respond to §512(c)(3) notices. SR hasn't sent any takedown notices.
- No inducement[?]. As discussed above, CMF's encouragement may weigh against it.

- Willful blindness. Although CMF does human content review and doesn't look for copyright infringement, I don't think this indicates (per Luvdarts) that CMF subjectively believes infringement is taking place and deliberately avoiding it. The knowing encouragement might, however.

On balance, I think CMF likely qualifies for 512(c), but it depends on how the judge considers CMF's encouragement of map uploads.

Section 230

I gave four examples of potential user-caused harms (beyond copyright) to evaluate:

- Abner's comments raise concerns about personal injuries and failure-to-warn.
- Billy's comments may be defamatory.
- Caleb's comments encourage the commission of federal crimes.
- Users may be misappropriating trade secrets, i.e., the proprietary GPS coordinates.

Prima Facie Case. Generally, CMF generally qualifies for Section 230(c)(1) for user-supplied content:

- ICS Provider. Websites qualify.
- Publisher/Speaker Treatment. Any claim based on user-provided content puts CMF into a publisher/speaker role of that content, unless a statutory exclusion applies.
- Provided by Third Party. User-provided content qualifies by definition.

CMF's human content review is irrelevant to Section 230.

Billy's Comments, Defamation, and Section 230.

Prima facie defamation case. Billy accusing Luke of illegal poaching may be defamatory:

- [False] statement of fact. *Bauer v. Brinkman's* considerations:
 - Definite/unambiguous meaning. "Illegal poaching" would be definite if there is, in fact, a specific crime against poaching. However, "poaching" can also be a colloquialism, i.e., fishers accusing each other of general misconduct.
 - Objectively capable of proof. If there is a specific crime on point, it's objectively capable of proof. If it's a colloquialism, then it's not.
 - Context around the statement. Online message boards are inherently filled with not-credible statements.
 - Social context. Fishers routinely exaggerate and tell stories. Also, if Billy and Luke are competitive rivals, Billy might be trying to kick a rival out of the market.
 - Conclusion: Whether this is a fact or hyperbole could go either way based on the provided facts.
- Of and concerning the plaintiff. It referred to Luke.
- Published to someone else. Posted online.

- Injurious to reputation. Allegations of illegal conduct are per se defamatory.
- Defenses. Illegal poaching could be a matter of public concern if it's sufficiently widespread. If it's one dude taking a few extra fish, it's probably not a matter of public concern. We don't have evidence about Luke's public figure status.

If the court treats Billy's statement as a statement of fact, it's likely defamatory. Nevertheless, per the Section 230 prima facie analysis, CMF won't be liable for Billy's defamation (promissory estoppel discussed below).

Exception: Roommates.com

Roommates.com said "If you don't encourage illegal content, or design your website to require users to input illegal content, you will be immune." As I explained in class, this applies if the site encourages/requires ONLY illegal content, which CMF didn't do. Users could upload comments of any nature, like the Roommates.com free-text box.

(It's true that CMF encourages uploads of proprietary GPS coordinates, but it also encourages uploads of freely available GPS coordinates too. I don't think the Roommates.com exclusion applies to those uploads).

Roommates.com also had an exclusion for materially contributing to content's alleged unlawfulness. I don't see that standard implicated in these facts.

Exception: Trade Secret Misappropriation (User-Uploaded Proprietary GPS Coordinates).

SR claims that proprietary GPS coordinates are its trade secrets. But trade secret protection only applies when information derives value from its secrecy. SR sells the coordinates once; after that, SR derives no further value from the coordinates' continued secrecy.

Even if SR has a prima facie trade secret claim against CMF, CMF can invoke Section 230. Section 230 does not apply to "intellectual property" claims. However, federal trade secret claims (DTSA) are expressly not "intellectual property" claims. Furthermore, any state trade secret claims based on user uploads will be covered by Section 230 in the Ninth Circuit (ccBill). The facts specify that all activity takes place in California, so the ccBill rule applies.

Some of you indicated that Section 230 preempts DTSA claims without mentioning the state law trade secret claims. In the Ninth Circuit, Section 230 applies to both.

Only about 40% of you discussed 230's trade secret exception.

Exception: Failure to Warn (Abner's Comment). Abner might be publishing inaccurate information that causes personal injuries, but CMF can generally invoke Section 230 to defend against any claims based on that. However, if an individual suffers personal injuries at the identified reef and sues CMF for failing to warn of Abner's known duplicity, Section 230 would not apply (*Doe v. Internet Brands*). However, odds are high that CMF doesn't owe any duty to warn, so the claim would likely fail despite getting around 230 (*Internet Brands*; *Beckman*).

Some of you wrote that Section 230 applies to offline injuries, as indicated by *Doe v. MySpace*. The Ninth Circuit created the failure-to-warn plead-around years after the MySpace case.

Exception: Promissory Estoppel (Luke). Luke can argue that CMF promised to investigate Billy's comments and never did so, so it should be estopped from disregarding its promise. Luke's promissory estoppel claim should get around Section 230 (*Barnes v. Yahoo*). However, it will fail on the merits. CMF only promised to investigate, not to take any action on the content. Further, Luke probably can't show that he detrimentally relied on CMF's promise.

Exception: Federal Criminal Prosecutions (Caleb's Comment). If users follow Caleb's advice, they could be prosecuted for illegal poaching. In theory, CMF could be prosecuted too, either for directly violating the crime (depending on the crime elements) or for aiding-and-abetting or otherwise materially assisting the criminal violation. If the U.S. DOJ prosecutes CMF, Section 230 categorically will not apply. However, CMF would have strong First Amendment defenses because it is simply publishing content. Furthermore, the Supreme Court's *Twitter v. Taamneh* ruling (issued after you submitted your exam) limits common law aiding-and-abetting claims. Despite Section 230's inapplicability, CMF is unlikely to be criminally liable for Caleb's comments.

Some of you conflated the Roommates.com "encourage illegal content" standard with the statutory exclusion of federal criminal prosecutions. For Roommates.com's purpose, "illegal" content means tortious content or content that violates state criminal law, because federal criminal prosecutions are already expressly excluded from Section 230.

ChatGPT's Sample Answer

[I ran the exam question through ChatGPT. I've included ChatGPT's response. It is riddled with errors and imprecisions and would not score well.]

Based on the information provided, here is an analysis of CatchMoreFish's legal risks:

Trademark Infringement: CatchMoreFish may be at risk of trademark infringement for using the phrases "Secret Reefs" and "SecretReefs" in its marketing and keyword advertising. This could potentially confuse consumers and create an impression of affiliation or endorsement with SecretReefs.

Copyright Infringement: CatchMoreFish allows users to upload GPS coordinates and associated maps, including those purchased from SecretReefs. If any of these uploads contain copyrighted material without proper authorization, CatchMoreFish could be liable for copyright infringement. Although they have implemented Section 512 protections and a repeat infringer policy, they should still take action upon receiving valid infringement notices to maintain their safe harbor protections.

Terms and Conditions Violation: CatchMoreFish obtained public GPS coordinates from SecretReefs' website by using an automated script, which is expressly disallowed by SecretReefs' terms and conditions. By disregarding these terms, CatchMoreFish may face legal consequences for breaching the terms of use.

Trade Secret Misappropriation: CatchMoreFish encourages buyers of SecretReefs' proprietary GPS coordinates to upload those coordinates and associated 3D maps. If CatchMoreFish knowingly solicits and accepts these uploads, they may be liable for trade secret misappropriation if SecretReefs can demonstrate that their proprietary information was misused or disclosed without authorization.

Negligence and Defamation: CatchMoreFish allows users to post comments about reefs, and while they review for profanity and nudity, they failed to investigate a potentially defamatory comment about illegal poaching. If CatchMoreFish's negligence in reviewing user comments leads to the dissemination of false information or defamatory statements, they may face legal liability for defamation.

Unfair Competition: CatchMoreFish competes directly with SecretReefs by offering similar services, using similar phrases in its marketing, and offering free access to public GPS coordinates that SecretReefs charges for. SecretReefs could potentially argue that CatchMoreFish's actions constitute unfair competition, particularly if they result in financial harm to SecretReefs' business.

It's important to note that legal risks can vary based on jurisdiction, and a more comprehensive analysis would require a detailed examination of specific laws and case precedents in the relevant jurisdiction. Additionally, this analysis is based solely on the information provided and may not encompass all potential legal risks associated with CatchMoreFish's activities.

[My followup query: Would CatchMoreFish qualify for Section 230?]

Based on the information provided, it is unlikely that CatchMoreFish would qualify for Section 230 of the Communications Decency Act (CDA). Section 230 provides certain liability protections for online platforms regarding third-party content posted on their platforms. However, there are several factors that may limit the applicability of Section 230 to CatchMoreFish:

Content Creation: CatchMoreFish appears to have an active role in creating and curating content on its platform. It allows users to upload GPS coordinates, maps, and photos, and it reviews user-submitted comments before they are publicly posted. Section 230 primarily shields platforms from liability for content created by third parties, not content that the platform itself actively participates in generating or selecting.

Lack of Good Samaritan Provision Compliance: Section 230 requires platforms to meet certain criteria to qualify for the law's liability protections, including compliance with the Good Samaritan provision. This provision stipulates that platforms must act in "good faith" to restrict access to or remove certain types of objectionable content. CatchMoreFish did not investigate a potentially defamatory comment and took no action on it, which could raise questions about whether they are meeting the good faith requirement.

Intellectual Property Infringement: Section 230 does not shield platforms from liability for intellectual property infringement. CatchMoreFish allows users to upload GPS coordinates, maps, and photos, and if any of this content infringes on someone else's copyrights, CatchMoreFish could be held liable for copyright infringement.

It's important to note that Section 230 is a complex and evolving area of law, and its application can vary depending on the specific circumstances and jurisdiction. A detailed analysis by a legal professional would be necessary to determine the precise applicability of Section 230 to CatchMoreFish's activities.