



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

This question drew inspiration from *Andersen v. Thompson*, 4:21-cv-08244-YGR (N.D. Cal. filed October 22, 2021), <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=3560&context=historical>. The court dismissed Andersen’s complaint in 2023 (with sanctions). *Andersen v. Thompson*, 1:22-cv-00627-DCN (N.D. Ohio July 14, 2023), <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=3824&context=historical>.

\* \* \*

**Anderson v. Morgan—Defamation**

*Statement of Fact.* Morgan said that Anderson “spied on rival searchers by surveilling them with drones.” The *Bauer v. Brinkman* factors help analyze whether this as a statement of fact or nonactionable opinion:

- Definite/unambiguous meaning. An accusation of “spying,” without more, has multiple meanings and could be a non-actionable opinion. However, Morgan included specifics that make the claim more definite and unambiguous, including the details that Morgan used drones and targeted rivals.
- Objectively capable of proof. The rival-surveillance-by-drone claim can be proven by showing that Anderson controlled drones, followed rivals, and acquired the resulting information.
- Context around the statement. Morgan made the statement on an online message board, which are generally rough-and-tumble. THOR in particular was known for conspiracy discussions, and it routinely traffics in hyperbole, exaggerations, and lies. This misinformation-rich environment increases the likelihood that readers do not believe what they read.
- Social context. The community norm against information stealing increases the believability of Morgan’s claim because it exacerbates readers’ paranoia and anxiety.

On balance, I believe Morgan’s rival-surveillance-by-drone claim was a statement of fact.

*Of and Concerning Anderson.* The claim specifically referenced Anderson.

*Published to Third Party.* Morgan communicated the claim to message board readers.

*Injury to Reputation.* Community members thought less of Anderson due to Morgan’s statement, as evidenced by the angry phone calls and mocking videos.

I believe Anderson has a prima facie case of defamation against Morgan.

*First Amendment Defense.* Morgan’s First Amendment defense probably won’t succeed. The public generally fears widespread drone surveillance, but this was a private surveillance of a few targeted individuals. Within the community of treasure hunters, news about a rival hunter’s “cheating” would be of substantial interest—especially with a winner-take-all prize, where cheating affects past and future investments by other treasure-hunters. Within the community, Anderson may have become a (limited) public figure due to the intense interest in the TS Consortium. Thus, I think the actual malice standard applies. However, Morgan has been reckless about the veracity of the factual claim. Morgan has no evidence suggesting Anderson did drone surveillance (other than perhaps an intuition). Without any basis for attributing the drone activity to Anderson, I believe Morgan has been both negligent and willful with respect to the fact’s veracity.

As a result, I believe Anderson’s defamation claim against Morgan would prevail.

[Note: in the defamation context, “actual malice” is a legally specific phrase referring to the speaker’s efforts to verify the factual accuracy of the claims. It does not refer to the speaker’s animus towards a person.]

### **Anderson v. Morgan—Direct Copyright Infringement**

*Copyrightability/Ownership.* Anderson likely owns the copyrights to the location photos that Anderson took and Morgan downloaded. (The TS Consortium might be the owner; I was fine if you analyzed it that way. TS might also have copyright interests in its “confidential details” if they express more than uncopyrightable facts).

*Registration.* We don’t know if Anderson registered the photos’ copyrights. Registration is required to sue, but it can be obtained right before suing. Non-timely registration would reduce Anderson’s potential remedies.

*Violation of 106 Rights.* Morgan downloaded and then uploaded Anderson’s photos to THOR, which constitutes a reproduction and distribution of the photos.

*Fair Use Defense.*

- Nature of use. Morgan’s use isn’t commercial, which favors fair use, but it’s not a non-profit educational use. Morgan didn’t transform the photos by adding anything new. Morgan’s animus towards Anderson signals the kind of bad faith that may affect the court’s consideration of the equities. All told, I think a court would count this factor against Morgan.
- Nature of work. The photos document factual information about the treasure’s location, which favors fair use. However, the photos were unpublished, which counts against fair use.
- Amount taken. Morgan uploaded 100% of each photo, which weighs against fair use.
- Effect on market for the photo. The photos are principally valuable because they document secret facts relevant to the treasure hunt. There’s probably no market for the photos if the associated location information were already publicly known. As photos of

secret information, Anderson only has a limited market for the photos because wider sales would undermine the secrecy and reduce the value to all buyers. Then again, courts would recognize Anderson's prerogative to keep the photos secret, and Morgan usurped that choice. Thus, I think most courts would weigh this factor against fair use.

Morgan's fair use defense will probably fail.

### **Anderson v. Morgan—Trade Secret Misappropriation**

A trade secret derives commercial value from being kept secret. The TS Consortium's purloined information about the treasure box location may qualify as a trade secret.

### **TS Consortium v. Morgan—Trespass to Chattels**

*Chattel.* The chattel is the TS Consortium's private server it owns.

*Chattel Usage.* Morgan used the server to download files.

*Authority.* If the server was open to the public, we'd assume the chattel owner impliedly authorized ordinary activity, including browsing and perhaps downloading, by voluntarily connecting to the public network. The TS Consortium's servers aren't publicly advertised but are publicly accessible. The servers didn't use password controls or other technological limits to override the default implied authorization. Thus, if the email to Morgan didn't indicate any access restrictions, Morgan legitimately may have believed that Morgan had the authority to access and maybe download the files. Alternatively, perhaps Morgan knew the servers were private (like Hamidi knew Intel employees' email addresses were confidential) or the tip email indicated some limits on Morgan's authority. We can't definitively resolve Morgan's authority to download files from the private server without more facts about Morgan's understanding.

[Note: some of you discussed Van Buren's "gates" metaphor. Collectively, your discussions of what constitutes a "gate" and when it's "up" or "down" were all over the map—a reminder that no one understands the metaphor.]

*Legally Cognizable Harm.* If Morgan's use was unauthorized, Morgan increased the TS Consortium's bandwidth cost for a month by an unspecified amount. We don't know if Morgan solely "caused" the overage or if other server users contributed.

- CFAA. The CFAA would recognize the bandwidth cost overage as a harm. The TS Consortium should win if the overage exceeded \$5k and is imputed to Morgan. If the overage was less than \$5k, the TS Consortium could make up the difference with any remediation expenses. However, if remediation simply means turning on readily available password controls, the additional remediation damages may be nominal.
- CA Penal Code 502. The overage should satisfy 502's harm requirement if it's imputable to Morgan.
- CA Common Law. Hamidi requires "measurable loss to computer system resources" to satisfy the California common law trespass to chattels requirements. Does the bandwidth

cost overage count? Hamidi said Intel didn't provide any "evidence [that] transmission of the messages imposed any marginal cost on the operation of Intel's computers." Here, the bandwidth cost overage constitutes a marginal cost to the TS Consortium. Yet, Hamidi's bulk emails surely imposed bandwidth costs and other marginal costs on Intel, and the court disregarded those. Maybe Intel didn't properly plead those costs? The Hamidi case would also recognize future threats of bulk downloads, but other downloaders are unlikely if the servers' URLs remain private. As a result, I believe that the California common law claim lacks sufficient harm.

If Morgan's access is unauthorized, the 502 claim and possibly the CFAA claim could succeed.

### **Anderson v. THOR—Defamation**

THOR republished Morgan's remarks, but Section 230 protects THOR from any claims based on those remarks.

*ICS Provider.* THOR is an online message board, a paradigmatic ICS provider.

*Publisher/Speaker Claim.* Defamation is a paradigmatic publisher claim.

*Third-Party Content.* Anderson's claim is based on Morgan's content.

The fact that THOR staff reviewed the uploads doesn't matter. This is an easy Section 230 case.

Anderson could claim that THOR didn't moderate Morgan's content out of anticompetitive animus. THOR and the TS Consortium/Anderson aren't direct competitors, but they both trade in information about the treasure hunt. The anticompetitive animus exception to Section 230 is so poorly defined that I don't know if it could apply here. I think it doesn't.

### **TS Consortium v. THOR—Section 230 and Trade Secret Misappropriation**

Section 230 protects THOR for Morgan's trade secret misappropriations despite the IP exception. A federal Defend Trade Secret Act claim doesn't qualify as an "IP claim" per the DTSA's definition. A state trade secret claim in the 9th Circuit is covered by Section 230 per *ccBill* (the opposite is true outside the 9th Circuit).

[Note: In the Ninth Circuit, Section 230 might preempt state copyright claims. However, state copyright laws only protect unfixed works, and (per *Cablevision*) almost all online works are fixed. If you said THOR could defend any of Anderson's copyright claims using Section 230, that was incorrect.]

### **Anderson v. THOR—Copyright Infringement and DMCA Compliance**

*Direct Infringement.* THOR doesn't directly infringe Anderson's photo copyrights because it's hosting Morgan's uploads and didn't act volitionally to violate a 106 right.

*Direct Infringer.* As discussed above, Morgan likely directly infringes Anderson's copyright.

### *Contributory Copyright Infringement*

- Knowledge of infringing activity. THOR may not know of the infringement. THOR staff reviewed the uploads, but the staff doesn't necessarily know which photos were infringing. Normally, a takedown notice would confer knowledge, but Anderson hasn't sent one.
- Material contribution. If THOR knew of the infringement, THOR's continued hosting of infringing uploads would materially contribute to the infringement.

I believe the contributory infringement claim would fail for lack of scienter.

### *Vicarious Copyright Infringement*

- Right/ability to supervise the infringing acts. Like other UGC services, THOR has the technical and legal capacity to review and remove Morgan's files. Usually, this factor requires something more. Would THOR's manual review of Morgan's uploads be that something more?
- Direct financial interests in the infringement. THOR doesn't directly profit from Morgan's infringement. At most, THOR benefits from drawing users to its site and encouraging more engagement with its offerings. *Napster* found impermissible financial interest when infringing items drew customers in, but THOR doesn't ordinarily use infringing items for that purpose, and THOR's monetization strategies don't relate to Morgan's infringement. As a result, the vicarious infringement claim should fail.

*Section 512 Defense.* If Anderson has a tenable copyright claim against THOR over Morgan's alleged infringement, THOR can invoke the 512(c) defense. THOR will not currently succeed with this defense. A quick look at the elements:

- Service provider: satisfied
- Store material at user's direction: satisfied
- Adopt repeat infringer policy: unknown
- Reasonably implement repeat infringer policy: unknown
- Communicate repeat infringer policy to users: not satisfied. The site terms and rules say that users agree not to violate the laws and that IP violations aren't allowed. I think this is too generic to count as a repeat infringement policy.
- Accommodate standard technical measures: N/A
- Designate agent at Copyright Office: not satisfied (no filings made)
- Post agent's content info on website. Not in the site terms and rules
- No actual knowledge or red flags of infringement. Satisfied? THOR's manual review of Morgan's material doesn't confer knowledge *of infringement* without other indications that the files are infringing.
- No right/ability to control infringement. Satisfied? This only occurs with respect to specific known instances of infringement, which isn't the case with THOR. Also, THOR

didn't exert substantial influence over Morgan to post infringing items (such as directing Morgan's behavior).

- No direct financial interest in infringement. As discussed above, I think this is satisfied.
- Exeditiously respond to 512(c)(3) notices. N/A because none sent yet.

THOR can qualify for the 512(c) safe harbor by adopting and implementing a repeat infringer policy and explaining it in its TOS. THOR also needs to designate an agent with the Copyright Office and post contact information on its website.

### **THOR Liability for Sticky Topics—Trademarks**

THOR incorporates TS Consortium's brands in four different ways: the sticky topic title, display of the logo, inclusion in the post-domain URL, and THOR's promotion of the sticky topic using keyword ads.

*Valid Trademark.* The phrase "Tesouro Sagrado" means "Sacred Treasures." Once translated, that phrase is either descriptive or suggestive for the TS Consortium's business. If it's descriptive, it would need to achieve secondary meaning to become protectable.

Although the consortium has high awareness in the treasure hunting community, it's not clear how the TS Consortium used the phrase in commerce, i.e., advertised or offered goods or services using the mark. After all, the consortium is still hunting the treasure. The TS Consortium will need to show that it used the term in commerce and, if necessary, achieved secondary meaning.

We don't have any details about the logo and if it qualifies as a protectable trademark.

*Priority.* If the TS Consortium used the phrase and logo in commerce, then it has priority over THOR.

*Defendant's TM Use in Commerce.* Per *Network Automation*, purchasing the trademark to trigger keyword ads is a use in commerce, as is displaying the phrase in the ad copy.

THOR's other activities depend on the applicable definition of "use in commerce." A sticky topic page isn't ad copy or product packaging; it's like a magazine referencing a trademark in an article name and showing the logo as part of the article. Per *Abitron*, THOR isn't using the TS name or logo to identify the source of its own goods. However, if use in commerce is coextensive with Congress' authority under the Commerce Clause, then THOR uses the mark and logo in commerce.

*Likelihood of Consumer Confusion Regarding Product Source.* THOR's sticky topic discusses the TS Consortium, but there's no reason for consumers to believe the TS Consortium is the topic's source. THOR could add a disclaimer, like *Lamparello* did, but I don't think it's necessary. The logo helps consumers identify the topic, but courts often punish logo usage. TS Consortium can invoke initial interest confusion, but I don't see how telling consumers that the site discusses the brand creates initial interest confusion. The *Lamparello* and *Network*

*Automation* cases indicate that the ad copy and the associated website must be considered together, essentially merging this discussion back into the standard likelihood-of-consumer-confusion analysis.

THOR used the trademark to trigger keyword ad and displayed the trademark in its URL. However, the second line clearly indicates that THOR provides the content, as does THOR's second-level domain name in the URL. A court may apply *Network Automation*'s 4-factor test:

- mark strength. The “Tesouro Sagrado” mark is relatively young but has some consumer awareness—enough that searchers are looking for it.
- actual confusion. No evidence of actual confusion, but a court might use IIC as a substitute.
- purchaser care. People interested in the treasure hunt are simultaneously gullible (prone to conspiracy theories) and extremely careful consumers of information.
- ad labeling. Google Ads are labeled as ads.

Per *Network Automation*, I don't think the keyword ad creates a likelihood of consumer confusion about product source.

[Note: some of you improperly flip-flopped between discussing the word mark and logo to analyze different test elements to achieve your desired outcome.]

*Nominative Use*. If the TS Consortium establishes a prima facie case of trademark infringement, THOR could claim the nominative use defense:

- THOR can't refer to the TS Consortium without using its brand.
- THOR had to use the brand to title the sticky topic, but did it need to include the logo? Did it need to include the name in the post-URL domain path? Courts might say that those uses of the TS Consortium's marks weren't necessary to identify the consortium. THOR could easily remove the logo without much downside, but changing the URL might be less clear to consumers. [Note: a necessary trademark use can qualify for nominative use even if other trademark uses took more than was needed.]
- THOR didn't suggest sponsorship or endorsement by the TS Consortium.

I think THOR will qualify for the nominative use defense for everything but the logo.

*Trademark Dilution*. The TS Consortium cannot show widespread national recognition of its phrase or logo.

[Note 1: the ACPA and UDRP apply to trademarks in domain names, not in post-domain name URLs.]

[Note 2: some of you conflated keyword ads with keyword metatags. They are different technologies.]

## THOR Liability for Sticky Topics—Section 230

THOR may face increased legal risk based on how it handles its sticky topics.

*Roommates.com*. Plaintiffs may argue that THOR partially develops content by manually creating sticky topics. This argument should fail. Service routinely taxonomize third-party content into topical categories, and that doesn't contribute to the alleged unlawfulness of any third-party content.

THOR could trip over a different *Roommates.com* exception if a sticky topic steered users to submit ONLY illegal content, such as a category titled “Breaking into top-secret government facilities” where users only discuss illegal ways of accessing facilities. THOR's sticky topic titles don't approach that line. For example, users can discuss both legal and illegal access in the “government property” topic.

*Negligent Design*. Could THOR be exposed to a *Lemmon v. Snap* workaround? Assume these claims are based solely on plaintiffs' behavior in response to the sticky topics, not any third-party content posted to the topics.

- Dangerous activity. Plaintiffs can argue that the “How Far Would You Go?” sticky topic motivates users to behave in risky, dangerous, and illegal ways. In other words, users might not just report on past activities but may undertake new activities to earn visibility and clout in the category. However, Snap allegedly had rewards keyed to higher speeds reported in the speed filter, but THOR doesn't provide rewards for users' activities. THOR's lack of a rewards system should distinguish *Snap*.
- Addictive behavior. Plaintiffs can argue that THOR's sticky topic addicts them to the treasure hunt. However, THOR doesn't addict users to THOR, which distinguishes it from the social media addiction cases.

Plaintiffs could allege THOR failed to properly warn them about the personal injury risks associated with the treasure hunts. That claim may get around Section 230, but it's unlikely to succeed on the merits.

*Federal Crimes*. The “Government Property” topic discusses federal crimes, as does the “How Far Would You Go?” topic. THOR cannot invoke a Section 230 defense against a federal criminal prosecution over those discussions. However, it's unlikely that THOR directly violates a federal crime by enabling user conversations of this nature. THOR's aiding-and-abetting liability would be governed by *Taamneh*, which likely favors THOR. THOR also could cite the First Amendment for enabling user conversations.

## THOR Account Registration Process

Applying my best practices guidance:

- Call-to-action visibility



- The call-to-action is left of the “complete signup” button, but the call-to-action and button are visually separated (they are on opposite sides of the screen).
- The call-to-action is the smallest font on the screen (virtually unreadable when printed).
- The call-to-action’s placement near the CAPTCHA box reduces defensible space.
- Call-to-action wording
  - The call-to-action lacks a conditional if/then statement, but the checkbox affirms user intent.
  - The call-to-action semantically conflicts with the CAPTCHA box, which also links to “terms.” Could consumers misunderstand what the “terms” refer to?
- Checkbox separate from and in addition to account formation action
  - The facts don’t specify that consumers must check the box to proceed. A mandatory checkbox cures some or all formation defects.
- Properly signal any TOS links
  - A small green font on gray background is hard to read. THOR doesn’t use the blue underlined links blessed by *Meyer*, which is slightly risky.
- No leaks
  - A mandatory checkbox should be leak-proof. However, THOR has legacy users who “leaked” into membership without agreeing to the terms.

Overall, if the checkbox is mandatory, I think courts would uphold THOR’s contract formation except with respect to the pre-TOS legacy users. If the checkbox isn’t mandatory, it’s a sign-in-wrap and probably still works, but the odds are closer.

THOR can easily improve its formation practices. Boost the call-to-action font size, give the call-to-action more defensible space, make the if/then condition clearer in the call-to-action, underline the hyperlink, and most importantly, make the checkbox mandatory. Also, force legacy users to click through the TOS to retain their accounts.

## ChatGPT's Answer

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

### (1) Claims against Morgan by Anderson and Tesouro Sagrado:

**Anderson's Claim:** Anderson could potentially have a defamation claim against Morgan for making false and damaging statements about Anderson spying on rival searchers with drones. However, Anderson would need to prove that Morgan's statement was false, that Morgan knew it was false or acted with reckless disregard for the truth, and that the statement caused harm to Anderson's reputation. Anderson may also need to show actual damages unless the statement is considered defamatory per se.

**Tesouro Sagrado's Claim:** Tesouro Sagrado and its consortium members may have a claim against Morgan for unauthorized access to their private server and the subsequent downloading and uploading of confidential information. This could potentially be a violation of trade secrets or computer trespass laws. However, Tesouro Sagrado would need to establish that the information downloaded by Morgan was indeed confidential and not publicly available elsewhere.

### (2) THOR's Legal Risks and Recommended Steps:

**Defamation:** THOR may face legal risks related to defamation if Morgan's posts are considered defamatory. To mitigate this risk, THOR should consider implementing moderation policies to monitor and, if necessary, remove potentially defamatory content. THOR should also remind users to adhere to community guidelines and avoid making false or damaging statements about others.

**Copyright Infringement:** THOR may be exposed to copyright infringement claims by hosting the materials uploaded by Morgan without permission. To mitigate this risk, THOR should implement a more robust review process for large uploads and ensure that copyrighted materials are not made publicly available without the owner's consent.

**Trade Secrets and Privacy:** THOR may face legal risks related to hosting confidential information from Tesouro Sagrado's private server. To mitigate this risk, THOR should promptly remove any uploaded materials that appear to contain trade secrets or private information. Additionally, THOR should consider implementing stricter content review processes to prevent the dissemination of sensitive information.

**Treasure Hunts:** THOR's treasure hunts involve participants paying money to participate. To mitigate legal risks, THOR should ensure that its treasure hunts comply with applicable gaming and gambling laws. Clear terms and conditions should be provided to participants, including disclaimers of liability for any harm or injuries that may occur during the hunts.

### (3) Legal Risks Associated with Sticky Topics and Account Registration:

Sticky Topics: THOR may face legal risks associated with the sticky topics discussing extreme measures, obsession, and potentially illegal activities. To mitigate these risks, THOR should consider reviewing and possibly removing topics that encourage or glorify illegal or dangerous behavior. Clear guidelines should be established for sticky topics to ensure they comply with legal standards and community standards.

Account Registration: THOR's registration process lacks terms of service, and some users registered before any terms were in place. To mitigate risks, THOR should implement comprehensive terms of service that clearly outline user obligations, community guidelines, and consequences for violating the terms. Users should be required to agree to these terms upon registration, and THOR should consider requiring existing users to acknowledge and agree to updated terms.

In conclusion, THOR should take proactive steps to review and strengthen its content moderation, user registration processes, and terms of service to mitigate potential legal risks associated with the actions of its users and the content they generate.

\* \* \*

[ChatGPT didn't discuss Section 230. As Gandalf indicated, that's an automatic F grade. I nevertheless asked ChatGPT if Section 230 would help THOR. ChatGPT responded:]

Section 230 of the Communications Decency Act (CDA) provides online platforms with immunity from liability for certain types of content posted by third-party users. Specifically, Section 230 states that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

In the context of THOR:

Defamation Claims: Section 230 could potentially provide THOR with immunity from defamation claims related to statements made by its users, including Morgan's posts about Anderson. THOR is generally not treated as the publisher of user-generated content, and therefore, it may be shielded from liability for defamatory statements made by users.

Copyright Infringement Claims: Section 230 may not provide absolute immunity for copyright infringement claims. Online platforms are generally not held liable for copyright infringement committed by users, but they may be subject to takedown requests under the Digital Millennium Copyright Act (DMCA). THOR should ensure it has a robust DMCA takedown process in place to promptly address any valid copyright infringement claims.

Trade Secrets and Privacy Claims: Section 230 is unlikely to provide immunity for claims related to the dissemination of trade secrets or private information. THOR may still be held responsible if it is actively involved in the unauthorized distribution of such content. Therefore, THOR should take proactive steps to remove sensitive materials promptly.

It's essential to note that while Section 230 offers a significant shield against certain types of legal claims, it does not provide absolute immunity, and there are exceptions to its protections. Platforms must still act responsibly and may face liability for their own actions or if they are directly involved in illegal activities.

In summary, Section 230 could potentially offer THOR some protection, particularly for defamation claims, but it does not provide a blanket immunity and may not fully shield the platform from liability for other types of legal claims. THOR should continue to implement and enforce content moderation policies and other measures to mitigate potential legal risks.