Santa Clara University

Internet Law (Law 793)
Final Exam Sample Answer
Prof. Eric Goldman • Fall 2017

Overview: This exam contains more issues than you had word count to discuss. Even with my pithy writing, my sample answer required over 4,000 words (before I added responses to student errors). With so many issues, you really wanted to use your word count budget wisely.

As usual, I encountered exams that underperformed because they: (1) addressed a few issues well (or at least competently), but missed other key issues altogether (such as exams—yes, plural—that did not mention Section 230 or Section 512 even once), or (2) spotted many of the right issues but provided little or zero analysis of those issues. I read each answer carefully looking for actual application of the law to the facts beyond recitation of the legal rules. Some answers simply never did that. I had to grade what the exam actually said, not what I might speculate you meant to say.

Here is my sample answer with comments on the student answers:

* * *

To: MakeADare CEO
From: Your favorite lawyer ☺
Re: Internet Law assessment and recommendations (Attorney-Client Communication)

[Ethics note: in practice, you should carefully consider the implications of providing a candid legal assessment in writing. You would mark the memo "Attorney-Client Communication" to reinforce that it should qualify for the privilege. However, you might still decide it's more prudent to conduct your debrief with the CEO orally.]

Liability for Member Content (Section 230)

There was so much to say about Section 230, and many of you said way too little about it. Reminder: it's not too late to get a tattoo of the statutory language!

Prima Facie Defense. Subject to exceptions, Section 230 generally eliminates all of our liability for members' videos/photos, comments, and other content they submit. We qualify for Section 230's immunity because:

- Provider/Member of Interactive Computer Service. Websites satisfy this element. [Grammar note: I saw too many butchered variations of the phrase "Interactive Computer Service." *Especially* on a take-home exam, it's inexcusable to use anything other than the correct statutory phrase.]
- Publisher/Speaker Claims. All suits against us based on member content will treat us as a publisher/speaker of that content unless it fits into one of the exceptions.

- Information Provided by Another Information Content Provider. We are not responsible for any content we did not create or develop (in whole or in part). This should apply to all content supplied by our members.

Thus, we do not face serious exposure for most member-caused legal violations. For example, if a member posts a video defaming a teacher through false accusations of sexual impropriety, we will not be liable for it.

Section 230 also protects us from liability for any personal injury that may occur due to a dare. We didn't discuss the case in class, but Maynard v. McGee [http://blog.ericgoldman.org/archives/2017/01/section-230-helps-snapchat-defeat-personal-injury-claim-due-to-speed-filter-maynard-v-mcgee.htm] held that Section 230 protected Snapchat from a personal injury claim by a victim of a car crash when the driver was using Snapchat's "speed filter."

RECOMMENDATION: Although we may not face legal liability, we should consider doing more proactive moderation of member-issued dares as a matter of trust and safety for our members. Many dares are so ill-conceived and dangerous that we have a moral responsibility to the community to scrub the worst dares. Section 230 will still protect us even if we choose to become more active moderators.

Section 230 has three statutory exceptions and numerous common law exceptions:

Federal Crimes Exception. Section 230 does not protect us against federal criminal prosecutions. Member content could violate federal criminal law in a variety of ways, such as the risk that any postings in the "sexual" category are child pornography. I'll discuss the child pornography risk in more detail below.

Federal Intellectual Property Exception. Section 230 does not protect us against federal IP claims (other than the Defend Trade Secrets Act). I'll discuss the federal copyright and federal trademark risks in more detail below.

State Intellectual Property Exception. In the Ninth Circuit, Section 230 immunizes state IP claims. Outside the Ninth Circuit, it doesn't.

We probably don't face much risk of publicity rights violations because most members' content will not have sufficient commerciality. However, member postings are likely to misappropriate trade secrets, such as the dare to show something your employer wouldn't want public. In class, we didn't discuss secondary liability for trade secret misappropriation. We don't have many cases on the topic. Most likely it would be governed by a notice-and-takedown rule.

RECOMMENDATION: If we're confident that we can't be sued outside the Ninth Circuit, we may not need to make any changes to address the risks from state IP claims over member content. Otherwise, at minimum, we should deploy a notice-and-takedown scheme in response to all state IP claims. We might also proactively delete any dares that we learn about that appear to request violations of state IP, especially trade secrets.

ECPA Exception. Members' recordings could violate the ECPA, such as surreptitious recordings of private conversations. However, it's unclear how we could be liable for republication of those videos, so we probably don't face much exposure from this exception.

Note: the exam facts indicated that you shouldn't talk about the ECPA, so I include this exception just for completeness.

Encourage Illegal Content (Roommates.com) Exception. Despite our admonishment to the contrary, many member-issued dares encourage illegal activity. Examples include the manspreader battery, the teacher defamation, the animal abuse, and the disorderly conduct by defecating in a public place.

However, the question is whether our site encourages illegal content, as opposed to what our members encourage each other to do. Because of Section 230, we should not be legally liable for what members say to each other.

However, MakeADare's categories possibly could qualify as encouragement of illegal content. All of the categories seem likely to generate potentially problematic dares and responses, but not all of them are automatically illegal. For example, the "food" category could involve completely legal activity (e.g., the "Paqui Carolina Reaper Madness One Chip Challenge Tortilla Chip"). Then again, so could the "pain" category, which might involve legal (if ill-advised) self-inflicted pain—such as the "pierce your own ear" dare, which is stupid but not illegal.

Viewed that way, the most risky category appears to be the "places you shouldn't be" category, which seemingly encourages other members to commit trespass. However, interpreted more broadly, it could involve legal but unexpected or risky spatial juxtapositions (say, a minority attendee at a white supremacy rally). So even topical submissions in this category could be a mix of legal and illegal content.

Even if a site category necessarily required illegal activity, it doesn't necessarily mean that the site "encouraged" illegal activity. As examples, I'll point to two cases we didn't discuss in class: Dyroff v. Ultimate Software, involving threads titled "heroin" [http://blog.ericgoldman.org/archives/2017/12/social-networking-site-isnt-liable-for-users-overdose-of-drugs-he-bought-via-the-site-dyroff-v-ultimate-software.htm] and Witkoff v. Topix, where the site established a category for "oxycodone" [https://www.forbes.com/sites/ericgoldman/2015/09/17/grieving-parents-still-cant-sue-topix-for-sons-oxy-overdose/#41c2ef0d69c3]. Both sites qualified for Section 230 despite these drug-specific threads.

RECOMMENDATION: rename categories to reduce the risk that they look like they encourage illegal activity, especially the "places you shouldn't be" category.

Other Roommates.com Exceptions. There no evidence that MakeADare materially contributes to any alleged unlawfulness of member content, such as by editing member content to make a true statement false.

Similarly, beyond the topical categorization discussed as part of "encouragement," there's no evidence that MakeADare structured/designed its site to advance illegal objectives. Though many dares are stupid, plenty of them are legal. Plus, Doe v. Backpage may have undercut this aspect of Roommates.com.

Failure-to-Warn Exception. Many member-issued dares will involve the risk of serious personal injury, including the bicycle, Pringles (risk of choking) and ear-piercing (risk of infection & more) dares. Failure-to-warn claims aren't covered by Section 230. However, they are also unlikely to succeed on the merits. (See the Dyroff case for more). Furthermore, we warned members that dares are risky, though our warning is quite general, without providing any specifics. If we have a duty to warn, our general disclosure might not be sufficient, though it would be impossible for us to enumerate the infinite number of specific ways that dares could pose a personal injury risk.

RECOMMENDATION: Though we probably aren't legally obligated to do so, we might make our warnings more detailed, more prominent, and more ubiquitous.

Liability for Member Content (Copyright)

We'll now turn to the IP exceptions to Section 230, starting with copyright.

Direct Infringement by Members. Members can commit direct copyright infringement in one of two principal ways: (1) members can copy material from elsewhere, and (2) the member content can incorporate third party copyrighted material, such as singing Katy Perry's "Peacock" song in a video.

Members can claim fair use for their activity. Each situation would have to be analyzed on its facts, but a few observations:

- If members copied 100% of a video or photo from elsewhere on the Internet, that will weigh against fair use (possibly heavily).
- Many members won't have a commercial motivation for their posting. However, if they posted to obtain karma, judges may still weigh the "purpose and character of use" factor against them because they are seeking a private benefit from the secondary usage. On the other hand, members who incorporate third party content into their dare video may have a decent transformative argument.

Note: every fair use analysis depends on the defendant's identity. Some of you discussed fair use without mentioning who was the defendant, and this is nonsensical.

MakeADare's Liability for Member Content. Assuming a member's video infringes and isn't fair use:

- Direct infringement. MakeADare should not be liable for direct copyright infringement due to its lack of volition. Cablevision.

- Contributory infringement. Ordinarily, MakeADare won't have the requisite "knowledge" of members' infringement absent takedown notices. Generalized knowledge that infringement could be taking place on the site won't qualify. Our karma incentive to members to incorporate music into their videos doesn't change this analysis because we don't try to motivate the incorporation of *infringing* music. Music could be original to the video uploader; it could be public domain music; or it could be licensed. If we get knowledge of infringement, we will materially contribute if we do not promptly remove the infringing item.
  [Note: some of you used the Grokster "induce or encourage" test for contributory infringement even though I mentioned in class that it's a minority test. Same with Grokster's vicarious infringement test.]
- Vicarious infringement. The legal standard for "right and ability to supervise/control" is nonsensical now. The Veoh case said it means "exert substantial influence on the activities of members." Arguably every member-generated content site does exactly that. We might have "direct financial interest" in infringement because our revenues (both from ads and merchandise) increase as the quantity of infringing activity increases, especially when we insert ads into infringing videos. On the other hand, our revenues increase from non-infringing activity, so we aren't trying to generate profits from only infringing activity. Still, we face a non-trivial risk of vicarious copyright infringement liability.
  [Note: "Veoh," not "Veho" ☹]
- *Inducement*. There is no evidence that MakeADare has the object of promoting site usage to infringe copyright.

Fair Use. MakeADare can assert a fair use defense independent of its members' fair use defense. Once again, the facts will depend on the specific case of infringement. However, the fact that MakeADare derives revenues from infringing activity will increase the odds that factor #1 (purpose and character of the use) weighs against it. We can counter-argue that, at least in some cases, the usage qualifies as transformative because of the site's focus on "dares" and the possibility that members added something new to the copyrighted material, like the video content surrounding the Katy Perry "Peacock" rendition. MakeADare's commerciality also increases the risk that factor #4 (market effect) will weigh against it, as courts may define a submarket for "dare videos/photos" and then circularly point to MakeADare's existence as evidence of the commercial viability of the market. While it's hard to discuss fair use in the abstract, it's not a sure-fire defense for MakeADare.

DMCA Safe Harbor. MakeADare may have a DMCA 512(c) defense for all material stored at members' direction. 512(c) would act as a complete defense against direct, contributory and vicarious infringement claims (Veoh).

First, we need to qualify for all the formalities. Note: on December 17, 2017, I did a search in the Copyright Office's agent designation database for MakeADare and Sparked and couldn't find a designation for either. So Step #1 would be to designate an agent ASAP!

Thereafter, the safe harbor should be available, and MakeADare should be liable only if we don't expeditiously respond to proper 512(c)(3) takedown notices. In particular, the Veoh case

indicated that the DMCA's "right and ability to control" element only applies to specific known instances of infringement, with that knowledge most likely being created by takedown notices.

Copyright owners could assert that we have willful blindness or red flags of infringement, but the stated facts don't provide any evidence of either.

Liability for Member Content (Trademark). Member content could depict or reference third party trademarks. The Pringles dare shows one of several ways that could happen; that dare is encourages consumers to misuse the product in ways that could lead to personal injury and damage the brand. For trademark infringement, the member would need to use the trademark "in commerce," which as indicated by the Lamparello case, is a murky standard when applied to editorial content like a gripe site or a stupid prank video.

Section 230 would not protect us from claims over members' trademark usage. However, we face contributory trademark infringement only when we "directly control/monitor the instrumentality used to infringe." Our hosting facilities may constitute that "instrumentality," but in the absence of takedown notices, ordinarily we will lack the required actual or constructive knowledge. Therefore, we should be able to manage our contributory trademark risk through a notice-and-takedown system.

While some member content might constitute trademark dilution, the lack of a contributory or vicarious dilution doctrine probably eliminates our risk.

Liability for Member Content (Child Pornography). Our site doesn't expressly encourage child pornography, but we face some risk of its presence, especially in the "sexual" category. The "Peacock" dare illustrates the risk. Though the dare doesn't indicate that one or both siblings must be underage, the dare could engender responses depicting one or more minors. Without Section 230 protection, default legal principles apply, as does the First Amendment. Our contract can tell members not to post child porn, but that contractual restriction won't end our legal exposure.

Note: the Child Online Protection Act was struck down as unconstitutional, so we don't face any liability from it.

RECOMMENDATIONS: We should get rid of the "sexual" category. Or, we could restrict posting to the category only by people who we've age-authenticated as adults, though this would be more costly to do and would not eliminate the possibility that depicted individuals are underage.

Considering MakeADare's audience and mission, I would prefer adopting a categorical "no nudity" policy, where we contractually restrict all nudity and remove any content containing nudity that we identify, whether it's from third party notices or we learn about it any other way. (If we discover child porn, we will also need to report it to NCMEC). We should investigate if there is cost-effective commercially available technology that can automatically filter out nudity.

COPPA. MakeADare may need to comply with COPPA. Doing so would be undesirable because of the out-of-pocket costs, other costs (such as extra engineering time), hassle factor, and risks of things going wrong. Therefore, we should ensure COPPA does not apply to us.

Appeal to Pre-Teens. The site is not "directed to" pre-teens. Some aspects are clearly oriented towards teens and adults, like the "sexual" category. However, other aspects may directly appeal to pre-teens, including the juvenile nature of "dares" and their associated humor, as well as the "schoolyard pranks" category. 16 CFR 312.2 provides some guidance about what the FTC considers to be "directed to" pre-teens, and I think a majority of the factors weigh against us being characterized as directed to pre-teens. However, COPPA applies to "portions of" a service directed to pre-teens, so even if our overall site isn't directed to pre-teens, we still have some potential risk.

RECOMMENDATION: Using the FTC guidance, we should do a thorough site review to identify aspects that might appeal to pre-teens and remove them.

Actual Knowledge of Pre-Teens. The account registration page contains a birthdate field. If registrations indicate an age under 13, we'll have actual knowledge of the registrant's pre-teen status. Actual knowledge of one pre-teen will force us to comply with COPPA.

RECOMMENDATION (in order of preference): (1) Eliminate birthdate field entirely. (2) Convert the birthdate field to age with pulldown menu including an option "under 18." (3) Reject account registrations from under 13s, and take steps to prevent immediate re-registration by bounced members.

Trademark Risks

Tagline Promotion. The tagline "Where YouTube meets *Jackass*" creates some trademark risk:

- Ownership of valid TMs. YouTube is a key trademark of Google. The "Jackass" trademark is presumably owned by MTV. Both trademarks are likely suggestive, not descriptive, and therefore immediately protected. (I believe both are also registered with the USPTO). Jackass is likely suggestive because it suggests an attribute of the service, i.e., the people depicted in the videos are acting like jackasses. Note that every descriptive trademark is, by definition, in the dictionary, but the line between generic and descriptive is whether the usage refers to the class of goods ("Apple" for the fruit) or a descriptor of the goods. Though the Jackass TV show ended a while ago, I'd be surprised if the trademark is abandoned due to other mark usages that have likely been made and are still being made.
- Priority. YouTube and Jackass have priority over MakeADare.
- Use in Commerce. The inclusion of the trademarks in MakeADare's ad copy and promotions qualifies as a use in commerce.
- Likelihood of Consumer Confusion. In the Silicon Valley, it's pretty common to describe new ventures as "Like X for Y," where X is a famous company and Y is a startup. [Check out new companies on AngelList and you'll see what I mean.] Stuff like "Like Uber, but for rickshaws" or "Like Airbnb, but for backyard treeforts." So in some consumer circles,

"Where YouTube meets *Jackass*" would be quite clear that YouTube and Jackass are analogous to, but different from, the company doing the promotion. In other circles, however, consumers might assume that the tagline refers to a Jackass channel on YouTube, or that Jackass has launched a service letting users publish their videos; or suspect some other sponsorship or affiliation between YouTube, Jackass and MakeADare. Also, I think the trademarks have substantial competitive proximity. YouTube, Jackass and MakeADare may cater to slightly different audiences, but they all publish videos of stunts. Combined with the possibility that consumers seeking out free dare videos won't be very sophisticated, there is some risk of consumer confusion about the service's source.

Even if the trademark owners could establish a prima facie case, MakeADare can claim that its references to YouTube and Jackass qualify as nominative use:

- There are not good synonyms for the YouTube or Jackass trademarks. (Note: some of you said that there are other ways for MakeADare to describe itself, but that's not the test).
- There's no evidence MakeADare took more than the one-word name references.
- The line "Where YouTube meets *Jackass*" does not directly suggest sponsorship or endorsement by either trademark owner, though consumers might still experience some confusion about the relationship between the three entities.

Overall, I think there's a good chance that the phrase qualifies for nominative use and therefore will not create liability. However, depending on MakeADare's risk tolerance, this phrase might be worth changing. If the phrase isn't generating strong marketing results, the legal risk may not be worth it.

YouTube is almost certainly a famous mark. Jackass may also be famous. If MakeADare qualifies for nominative use, that ought to qualify as a "fair use" for purposes of the dilution defense. Even if it doesn't, it's hard to see how MakeADare's reference to YouTube and Jackass would constitute blurring, because it doesn't add new definitions to the terms. The risk of tarnishment is also low, though perhaps MakeADare's "sexual" category would create a slight risk.

Keyword Advertising. All of the prior trademark analysis applies, but with the following twists:

- It's pretty well accepted that buying trademarked keywords constitutes a use in commerce of those trademarks, but that's irrelevant here because inclusion of the trademarks in the ad copy also constitutes a use in commerce.
- The ad copy "We dare you to join us" raises some questions about who "we" and "us" refers to. Is it MakeADare, YouTube, Jackass, or some combination thereof? The ad copy's reference to the makeadare.com URL might clarify that "we" and "us" refers to it. To me, this is analogous to the Network Automation case's reference to "networkautomation.com" URL in its ad copy. If consumers know the set of competitors, this disclosure is clear. If consumers don't know those brands, however, they have no reason to assume that MakeADare is unrelated to YouTube or Jackass.

- If YouTube or Jackass complain to Google, Google will block the current ad copy because of the incorporation of third party trademarks. We probably don't fit into any exclusion to Google's policy. For example, we're not an "informational site" about either YouTube or Jackass.
- The keyword ads create an additional risk of exposure to initial interest confusion. In light of Lamparello, and following Network Automation, the initial interest confusion analysis should consider the ad copy in conjunction with the MakeADare site—which, upon initial visual inspection, pretty clearly has nothing to do with either YouTube or Jackass. Therefore, it's unlikely initial interest confusion will create any extra risk of liability.
- Furthermore, per Lens.com, the court may use clickthrough rates to measure actual confusion, and that weighs heavily in our favor.
- Network Automation highlighted four factors to consider, three of them from the Sleekcraft case. The fourth factor is the labeling of the ads as ads. If Google adequately labels its ads (admittedly, this remains debatable), trademark owner cases over keyword ads are even less likely to succeed.
- Keyword advertising buys don't constitute dilution. *See* Allied Interstate LLC v. Kimmel & Silverman P.C., 2013 WL 4245987 (S.D.N.Y. 2013); Designer Skin, LLC v. S & L Vitamins, Inc., 560 F. Supp. 2d 811 (D. Ariz. 2008); Nautilus Group, Inc. v. Icon Health & Fitness, Inc., 2006 WL 3761367 (W.D. Wa. 2006); Edina Realty, Inc. v. TheMLSonline.com, 2006 WL 737064 (D. Minn. 2006).

RECOMMENDATION: Though the tagline and keyword ads are probably legally OK, we would not want to spend much money defending our right to use them. We should investigate how effective these references are for us and whether their value justifies the potential costs we'd incur if we have to defend them. Otherwise, we might be better served allocating our marketing dollars elsewhere.

Note: some of you discussed keyword metatags even though the facts contained nothing to support that discussion.

Contract Matters

Formation (account registration). The account registration contract formation probably works legally, but it's old-school.

Call to action language: "I agree to the Terms and Conditions" unambiguous indicates that consumers are manifesting assent, but it would be better stated as an "If/Then" statement about how they are manifesting assent, i.e., "By clicking the 'Submit' button, I agree to the Terms and Conditions."

Call to action placement: the placement immediately above the submit button is good. However, the grey box shading, especially with the small grey font, keeps the call to action from standing out. The font should be bigger, the font should be in black (not grey), and the shading should be removed or should changes to a color that highlights the language.

Other attributes: Nowadays, we'd prefer a checkbox, in addition to the submit button, to make sure courts recognize this as a clickthrough/"clickwrap." It would also be preferable to display at least some of the terms on this page, perhaps between the call to action language and the submit button. We need to confirm that there is no way for members to create an account other than by clicking through this page.

Despite the old-school implementation, the legal test is whether a consumer manifests assent to the terms. I believe most courts will find this implementation is effective as demonstrating consumer assent to the terms.

RECOMMENDATION: We should refresh the contract formation process to modern specifications. Improve the call to action language, improve the display, add a checkbox and preview of the terms.

One quirk: MakeADare's CAPTCHA vendor includes a "privacy and terms" link for its CAPTCHA service. This has several downsides. Potential members might think this link is redundant with our links; so consumers who view this link might have genuine confusion about whether the CAPTCHA link's terms are the only terms applicable to our relationship. Also, potential members might be confused by which link the call to action refers to.

RECOMMENDATION: If we implement the other recommendations, we solve most of the problems. However, we should work with the CAPTCHA vendor to eliminate the "privacy and terms" link entirely, and if that's not possible, we may want to switch CAPTCHA vendors.

Formation (non-account registration). MakeADare has two other ways we might claim contract formation with non-account registrants. First, its footer contains a link "Terms and Conditions." This is almost certainly not enforceable—it's not even a "browsewrap" because it does not have a call to action indicating that browsing constitutes assent.

Second, the terms and conditions expressly say that "by viewing and/or using this web site, you agree" to the terms. This language is almost certainly not enforceable either. Most consumers will never see this language, and their onsite activity doesn't unambiguously manifest assent to the terms.

Thus, MakeADare probably doesn't have any binding terms with non-members. However, so what? What legal risks does MakeADare face to non-members? Perhaps the biggest would be to discourage viewers from imitating dares, but this could be done through onsite warnings that don't require contract formation (indeed, burying the warning in a contract would reduce its prominence). Otherwise, I can't think of any meaningful risks that MakeADare needs to control with non-members.

RECOMMENDATION: If MakeADare thinks it needs a binding contract with non-accountholders, it needs to change its implementation radically. However, I don't recommend pursuing that option because there is no real legal risk with viewers that needs to be managed via contract.

Amendment. The terms and conditions contains the ubiquitous but legally dubious statement that contract changes can be made by posting them to the website without further notice to members. As indicated in the Blockbuster case, this language probably doesn't work; and it potentially jeopardizes the entire contract's validity.

RECOMMENDATION: Specify that any contract amendments will be made only after notice is given to members, perhaps through email or onsite notifications.

Member Server Misuse

The unwanted member activity damages the site's community, but the odds we'd actually sue any of our members is near-zero because it would spook other members and any court-issued remedies aren't likely to be worth their cost. Therefore, suppressing unwanted member activity is almost certainly a technological and member relations challenge, not a legal one. Still, for the sake of completeness, I'll run through the legal doctrines that protect our interest.

Common Law Trespass to Chattels. Members use MakeADare's chattel to send private messages and create fake accounts. The private message limitation is expressly communicated in the onsite disclosure, making the use unauthorized. It's not clear if/how the technical limits on the number of message recipients are communicated, so MakeADare may not have successfully communicated that those activities are unauthorized. However, members proliferating fake accounts apparently have learned about the limits, at least implicitly. To the extent there is any ambiguity about their knowledge, we can remove that ambiguity by sending cease-and-desist letters to them.

Under the CA rule, we'd have to show such activity has caused a measurable loss to our system resources. As annoying as these activities may be, we may not be able to show that they have degraded the technical capacities of our network. The 50 message limit makes it hard for any individual member to generate much server usage.

Under the majority rule, we'd need to show some harm. The Restatements harm includes impairment of the chattel's condition/quality/value, though we don't have much evidence of this. We do have evidence that such activity has harmed our goodwill with other members, and this might qualify as harm to a legally protected interest. We can also show that we've exercised self-help via our imposition of technical limits. The likelihood of follow-on members engaging in similar practices is demonstrably high here, though the aggregate consequences of all follow-on activity still may not be enough to jeopardize our network's integrity.

All told, this is not a slam-dunk case for common law trespass to chattels, but we have some good arguments that might prevail.

CFAA. We can show that members have knowingly transmitted information, and intentionally accessed our network, without authorization. We can further show that their activities have harmed us over $5,000 per year by counting our efforts to impose new technical limits and to find and suppress fake accounts. Therefore, we likely have a good CFAA case.

CA Penal Code 502. Members have used and accessed our network, and that activity imposed verification and remediation costs on us. Therefore, we likely have a good 502 case.

CAN-SPAM. Our provision of a private messaging service qualifies us as an Internet access service, and the private messages could constitute impermissible commercial electronic mail messages if we can find the requisite commerciality. The pursuit of karma on our site is a non-financial reward that ends the CAN-SPAM case. However, some members can convert their higher site visibility into cash, in which case their private promotional messages might constitute commercial spam. In that case, we'd have another legal basis to pursue members.

Overall, we have multiple legal doctrines that should allow us to sue members for their promotional private messages and fake accounts if we chose to pursue them in court; and we likely don't need to make any changes to improve our litigation position. Still, because we're not going to sue our members, we need to find other ways to curb this behavior.

RECOMMENDATIONS: We should do more to block members from creating multiple accounts. We might consider changing the karma system to reduce its incentives for unwanted behavior.