Internet Law

Professor Grimmelmann

Final Exam - Fall 2012

I graded each essay question using a checklist, giving a point for each item (e.g., "Under *Drew* and *Nosal*, violation of Ops' terms of service is not a violation of the misuse statute") you dealt with appropriately. Ten percent of the credit in each each question was reserved for organization and writing style. I gave bonus points for creative thinking, particularly nuanced legal analyses, and good use of facts.

Model answers to the three questions are below. I recommend that you compare your essays with them. The model answers aren't perfect; no answer in law ever is. Indeed, it was frequently possible to get full credit while reaching different results, as long as you identified relevant issues, structured your analysis well, and supported your conclusions.

If you would like to know your scores on the individual essays, have further questions after reviewing your exam, or would like to discuss the course or anything else, please email me. It will be hard for me to meet in person this semester, but I will be happy to talk on the phone or via Skype.

It has been my pleasure to share the past semester with you, your enthusiasm, and your insights.

James

	Major Crimes	Barksdale	Bubbles	Total
Median	15.5	14.5	15.0	44.0
Mean	15.8	14.9	14.7	45.4
Std. Dev.	5.2	4.0	5.1	12.5

(1) Major Crimes

Obscenity

Assuming that the promotional emails from JayLBait do not themselves contain obscenity or child pornography, it is not currently possible to prosecute Burrell and the Floridian John Doe for their use of the site. We could attempt to charge them for "distributing" obscenity: the story in the drafts folder. It appears to satisfy the *Miller* test: it appeals to the prurient interest, it is patently offensively sexual, and there is no indication that it has serious literary value. The use of Maryland community standards is not problematic under *Kilbride*. Given Burrell's presence in Maryland and his one-on-one dealings with Doe, prosecuting either of them would not create the same problem of overlapping inconsistent standards discussed by *Kilbride*. The defendants might claim that they did not "distribute" the story because it always remained a draft. But it appears that they were using the draft to communicate with each other, which should count as a distribution. (*Cf. London-Sire*.)

Child Pornography

We probably cannot charge Burrell or Doe with possession of child pornography. While the story describes the sexual abuse of a minor, it does not satisfy either of the justifications given in *Free Speech Coalition*. The story does not depend on the actual abuse of an actual child, as pornographic films and pictures do. And assuming that the story has remained secret, it does not extend and repeat the victimization of an identifiable child.

Threats

We probably cannot charge Burrell and Doe under a Maryland equivalent to 18 U.S.C. § 875(c) for making threats to injure another. As in *Baker*, the story is probably not a "true threat": it was not communicated to the potential victim, nor did it appear to describe an imminent risk of

violence. The fact that Burrell and Doe drafted the story over the course of weeks, and the fact that Doe is an unknown Floridian, imply that the story is not the record of an actual plan to abduct and murder James McNulty. The initials suggest that it may refer to him, but the age difference suggests that it may not. The story (if we had obtained access to it legally) might provide probably cause for further investigation, but I doubt that it is sufficient to obtain a conviction.

Computer Misuse

We probably cannot charge Burrell and Doe under the Maryland computer misuse statute. The only potential theory under which they accessed a computer without authorization or exceeded authorized access to obtain information (the story), § 1030(a)(2)(C), is that their access was unauthorized because it was in violation of the Ops terms of service. They violated clause 8 by sharing a single account and password; they violated clause 10 by distributing illegal obscenity to each other. Whichever of Burrell and Doe created the account explicitly clicked through the terms of service, which is sufficient to make them enforceable. *ProCD*. If the other tried to argue that he had not agreed to the terms, then he would be using the service without any authorization at all (except from his partner, which was explicitly prohibited out in the terms of service). Unfortunately, under *Drew* and *Nosal*, violation of terms of service is not sufficient to constitute a lack of "authorization."

JayLBait

The BPD did not violate the Fourth Amendment by obtaining JayLBait's customer records from Landsman. Under the third-party doctrine, as in *Miller* (discussed in *Warshak*), the emails addresses were voluntarily shared with JayLBait and was necessary for its employees to access in the ordinary course of business. He may have violated § 2701(a)(3) of the Stored

Communications Act by disclosing customer records without sufficient legal process. I will need to know more about his plea agreement to reach a more definitive conclusion.

Ops.com

The Fourth Amendment protects the draft email. *Warshak*. The fact that it was not sent as an email only heightens the protection: Burrell and Doe took even more stringent steps than Warshak did to keep their communications confidential. Thus, the BPD could only obtain the contents of the account with a search warrant. While Detective Moreland likely had probable cause to obtain a search warrant, he did not do so, relying instead on the lesser "specific and articulable facts" standard of a (d) order. Just as in *Warshak*, the Fourth Amendment exclusionary rule applies—but unlike in *Warshak*, the good faith exception will not apply, as *Warshak* is now on the books.

Detective Moreland didn't even execute his request correctly under the Stored Communications Act. A (d) order is only an option under § 2703(b), for communications stored more than 180 days. The drafts each day were in storage for less than 180 days, requiring the use of a warrant, as specified in § 2703(a). (We could dispute whether the drafts were "electronic communications" that were in "electronic storage" in the first place, given that they were never "sent," but taking a functional approach, they are the equivalent of email in every way.)

There is also potentially a Wiretap Act issue here, because Ops enabled Moreland to engage in ongoing surveillance of the deputy account. Assuming that the drafts were "electronic communications," it appears that they were "intercepted" because Ops enabled Moreland to view their contents. The harder question is whether this once-a-day method of disclosure satisfies the contemporaneity requirement discussed in *O'Brien*. Here, the interception was arguably not simultaneous with the message's transmission but rather a day later. But it is possible that

capturing the drafts for later inspection might constitute an interception. In light of the Fourth Amendment problem, this is probably a moot question.

Recommendations

Since the surveillance of the Ops account will be subject to the exclusionary rule, the obscenity prosecution over the draft email is likely impossible. The account information—the IP addresses—is another matter. That was properly disclosed under a (d) order, § 2703(c). We do not have enough evidence to charge Burrell and Doe now, but the subscription to JayLBait from identified IP addresses is probably sufficient to obtain a search warrant for Burrell's Towson address. Detective Moreland should search Burrell's computers in hopes of finding him in possession of child pornography. (There is a risk, however, that a court might sweep in the IP addresses as fruit of the poisonous tree, on the theory that Moreland was motivated to search Burrell's house by learning of the story.) It is possible that Burrell has been misidentified—IP address identification is imperfect, someone else could have been using his WiFi connection, etc. —but that should not stop us from obtaining a search warrant.

I will contact my counterparts in Florida law enforcement to discuss the possibility of a simultaneous search of Doe's location. We may be able to prosecute Doe in Maryland if we can link him to the Maryland-based JayLBait. If not, there are almost certainly potential Florida criminal charges available for those found in possession of child pornography.

(2) The Barksdale Organization

Copyright

It is not clear whether Corner Boys or barksdaleorganization.com are user-generated-content sites or whether their operators posted all of the content on them. I will assume the latter; if not, a similar analysis to that I will give below for Hamsterdam would apply to them.

Corner Boys and barksdaleorganization.com are direct infringers of the reproduction right because they each have unauthorized copies of the Barksdale Organization's copyrighted sound recordings. (I will leave aside the threshold issues of fixation, copyrightability, and copyright formalities, all of which I will assume are satisfied.) They are also likely direct infringers of the distribution right. Under the reasoning of *London-Sire*, the inference that some users have actually downloaded the sound recordings is highly plausible, given the links from Hamsterdam. Any user who downloaded the recordings from one of these sites is likely to have infringed the reproduction right.

It is unlikely that these sites or the users could avail themselves of an implied license defense. Contrary to SuperMarloBros's theory, the Organization's permission to listen to all of its recordings for a $25/year fee and putting online the most recent recording for free do not translate into permission to copy them all freely. *AFP v. Morel*. The fair use claim for this acts of infringement—the unlimited distribution of unmodified complete recordings in competition with the Organization's own subscription service—is also weak. *Napster*. PartLowPartHigh's arguments do not explain why he should not be expected to pay for access to the music he is enjoying online. If he has a claim under the ADA, it is against any inaccessible jazz clubs the Organization plays at, not against the Organization itself.

Hamsterdam (i.e. the Colvin Media Group) could be secondarily liable for linking to these infringing files. It is not a vicarious infringer on the facts available to me; while it can arguably control the infringement by deleting links, it has no direct financial benefit from the infringement. (I could examine the site more closely to understand its revenue model.) It is potentially a contributory infringer: it contributes to the infringement by linking to it, and it has at least general knowledge of ongoing infringement. The key is that unlike Sony, it provides a service, so that by giving Hamsterdam notice of specific acts of infringement, you could hold it liable if it failed to take action. *Napster*. It is not an inducing infringer on the available facts: nothing it has done has the deliberate intention of fostering infringement.

Hamsterdam, however, probably has a defense under the § 512(d) safe harbor for linking to infringing content. I will need to examine the site's DMCA policy and compliance, but the most that you will be likely to be able to do is to send Hamsterdam DMCA takedown notices to remove specific links to your files from its forums.

Barksdaleorganization.com Domain Name

The domain name barksdaleorganization.com consists of the name under which the Organization performs and does business; it may be a trademark of the Organization (or, to be pedantically precise, a service mark). This would let you sue the unknown principals behind the site for trademark infringement and cybersquatting under the ACPA. There does not appear to be a bona fide use of the—indeed, it seems to be used to advertise for infringing materials, using the exact trademark itself. In addition, the site's use of false contact information in its registration will count against it.

The ACPA, however, may be serious overkill against a hard-to-find defendant. You will get better and faster results from bringing a UDRP action, which is likely to succeed for similar

reasons. The remedy would be transfer of the domain name: you could use barksdaleorganization.com yourself for the group's homepage if you want.

Counterfeit Tickets

Selling forged tickets with the Organization's name on them is potentially a trademark violation. If so, then the standard from *Tiffany* would apply: Hamsterdam is not liable for its users' infringing items for sale unless it has specific notice and fails to act. You should send Hamsterdam notices about tickets that are obviously fraudulent, such as those for shows that have not gone on sale yet. For other tickets, it will be harder for you to detect whether they are genuine or not; I suggest you post a warning on your own website and in the forums at Hamsterdam, and talk to Colvin about taking its own enforcement actions against sellers who turn out to have been lying. (They should want their marketplace to be clean, just as much as you do.)

To the extent that these fake tickets violate other state laws, such as prohibitions on scalping and fraud, Section 230 will probably preempt any liability on Hamsterdam's part. While we could argue that liability here would attach not to Hamsterdam as a speaker but for its role in facilitating fraud, the *MySpace* court rejected a similar argument as "artful pleading."

User Abuse

Hamsterdam is absolutely immune under Section 230 from being held liable for the harmful speech of its users. You probably do not have any valid claims against the users, anyway. CheezIt's statement of opinion is protected by the First Amendment because it is subjective, not provably true or false. And da_snoop's plan to "hunt [Avon] down" is probably too vague to qualify as a "true threat."

Practical Issues

Any suits against users will face the usual challenges in identifying them: multiple subpoenas, a long and possibly contested discovery process, and the possibility that the IP address trail will grow cold or take a wrong turn. Jurisdictionally, there shouldn't be much trouble bringing suit against Colvin if we are willing to go just up the road to New York. CornerBoys could almost certainly be haled into court there, thanks to the New York long-arm statute's application to deliberate copyright infringers as seen in *American Buddha*. barksdaleorganization.com is located who knows where and is a low-value target to pursue.

Advice

I strongly recommend that you not sue users of any of these sites. Indeed, filing any lawsuits is not likely to go over well with your fans and may harm your relationship with them, on which the Organization depends. (Witness how well they responded to your chiding in the Hamsterdam forum.) One possibility is to use DMCA notices to take down the links but not to escalate to a lawsuit. You could also continue the conversation with the users to make clear that you depend on revenue from the Pit to be able to continue working as a band, while asking them what you could do to convert these downloaders into paying users. (If you're still making $50,000 a year from the Pit despite these bootleg sites, the news can't be all bad.) Where you should act most aggressively is in response to the counterfeit tickets: those are very bad for your fans, for whom you should stick up.

(3) BubblesDepot

CFAA

Bubble's theory of liability under the CFAA faces one huge obstacle: authorization. The BubblePhone is a "computer" as it is a electronic device, and anyone who runs Prezbify necessarily accesses it to install Prezbo. Prezbo users who run Prezbify own the BubblePhones on which they install Prezbo. As an owner of a BubblePhones, a user can authorize herself to access it. By providing Prezbify to users, Prezbo itself accesses nothing. (Prezbo presumably owned all of the BubblePhones it used to develop Prezbify, so a similar conclusion applies.)

Bubble would argue a lack of authorization under the *Morris* "intended function" test. The function of Developer Mode is not to install programs. But we could respond that Developer Mode is intended to allow troubleshooting and the suspension of normal restrictions on how apps are installed on a BubblePhone. A terms-of-service theory of lack of authorization would fail in light of *Drew* and *Nosal*.

Bubble's best argument is that Prezbo violates § 1030(a)(5)(A)'s prohibition on transmitting a program that causes damage when it provides Prezbify for download. But even this argument has problems. For one thing, this prong of the CFAA requires "damage" to the computer: if anything, the computer has been enhanced from its owner's perspective. The only "impairment to the integrity . . . of a program" is that the BubblePhone now has Prezbo.

Section 1201

Bubble has a stronger argument under Section 1201. The technological measure is the software lock in BubsOS that prevents installation of apps without a Bubble-provided key. In its ordinary operation, it requires a Bubble-supplied key. This measure protects access to two kinds of copyrighted works: the music and apps that users install on their BubblePhones, and BubsOS

itself. An argument that this protection is not "effective" would probably fail. The fact that Developer Mode is undocumented and used only for troubleshooting suggests that in the ordinary course of use, a BubblePhone will never be placed into Developer Mode. A court following *Remeirdes* would consider this effective enough.

A user who runs Prezbify circumvents this technological measure by disabling the need for a key to install an app, in violation of § 1201(a)(1). By distributing Prezbify, Prezbo violates § 1201(a)(2). Prezbify is designed to get around the need for a key, as in (a)(2)(A); its only use is to avoid the need for a key, as in (a)(2)(B); and Prezbo marketed it specifically to get around the restrictions on BubblePhones, as in (a)(2)(C).[1] It doesn't matter that Prezbo is a noninfringing use: per *Remeirdes*, a DMCA violation can occur even without copyright infringement.

Copyright

Prezbo allows users to stream music to each other. These streams may be infringing public performances under *Cartoon Network*. Certainly if a user streams the same music to more than one other user, it would be a "public" performance. Outside of the Second Circuit, it is possibly a public performance even if it goes to only one other user. The users might have a fair use defense: while they're sharing complete songs unaltered, their inability to keep permanent copies (unlike in *Napster*) reduces the market impact of the sharing.

Prezbo is not a vicarious infringer, at least not on the facts before me, since it is not clear that Prezbo can control when and how users stream music to each other once they download the software. It has a *Sony* defense to contributory infringement, as users could use this feature to stream public-domain music to each other. The biggest concern might potentially be inducement

---

[1] Some of you pointed to the Library of Congress rulemaking exemption for jailbreaking smartphones to install unauthorized apps. But note that the exemptions only apply to § 1201(a)(1), not to § 1201(a)(2), so Prezbo isn't off the hook.

infringement—the invitation to users to "start showing off your taste in music" could be construed as an invitation to infringe. Fortunately, Bubble is unable to raise this claim itself, as it is not the owner of the copyrights in the music that users share.

Antitrust

Prezbo's best counterclaim is that Bubble is violating the Sherman Act by attempting to monopolize the social network market. As in *Microsoft*, Bubble is tying its BubbleSocial product to its BubblePhone product, and using technological and contractual restrictions to prevent the installation of competing social networks. In this analogy, BubbleSocial is Internet Explorer, the BubblePhone is Windows, and Prezbo is Netscape. The restriction on installing Prezbo, enforced via the need for a key (which Bubble has refused) is anticompetitive because it inhibits Prezbo's ability to reach consumers on the BubblePhone platform, preventing its social network from achieving critical mass and reducing its ability to compete with BubbleSocial. Bubble can offer some pro-competitive justifications for the restrictions it creates, such as improving the user experience for BubblePhone owners. But by rejecting Prezbo under such clearly inappropriate guidelines as "no fart apps," Bubble undercuts its own argument that the restriction has benefits for users.

Bubble does, however, have two powerful replies. First, there is probably the doctrine, seen in *LiveUniverse*, that it has no duty to assist its competitors. And second, Bubble does not have a monopoly in the smartphone market, as it is only one of three major competitors.

Miscellaneous

Prezbo cannot hope for help from the FCC under the Open Internet Order. Even if Bubble is considered to be providing broadband Internet (rather than the cellular carriers on whose

networks the BubblePhone runs), Prezbo is not an application that competes with Bubble's "voice or video telephony services."

Prezbo has no affirmative First Amendment right to reach users of BubblePhones. *Cyber Promotions*. Bubble can also argue in its defense hat it has a right under Section 230(c)(2) to screen out objectionable content, including apps. But Prezbo might be able to respond that Bubble's false public statements about the rejection's basis could constitute tortious interference with contract. Bubble has falsely represented to the world that Prezbo is a fart app and isn't up to Bubble's standards of quality. But then again, Bubble might claim that its "standards of polish and quality" are purely subjective, as in *Search King*.

The Bubble guidelines might not be an enforceable contract because they do not appear to impose any obligations whatsoever on Bubble. In any event, they cannot constitute a defense to Prezbo's antitrust claims, because antitrust law itself prohibits contracts in restraint of trade.

Advice

Bubble's Section 1201 argument is strong enough that I suggest we disable Prezbify while we resolve this situation. But our antitrust counterclaim may give us some leverage. I suggest that we take down Prezbify while putting up a blog post telling our side of the story (including Bubble's ridiculous explanations) and explaining to our users how Bubble is bullying us off the BubblePhone and hinting that we are considering filing an antitrust lawsuit. The public attention might be enough to cause Bubble to relent.