Internet Law

Professor Grimmelmann

Final Exam - Spring 2011

I graded each essay question using a checklist, giving a point for each item (e.g., "Lucille receives a life estate.") 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.

Almost all scores fell between 5 and 25 on my scale, as did the scores for your forum posts, so I added them together to produce an overall score on a 100-point scale.

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 and for your overall forum posting, please ask my faculty assistant, Alexzia Plummer, in the IILP offices on the 9th floor of 40 Worth St. If you have further questions after reviewing your exam, or would like to discuss the course or anything else, please email me and we'll set up an appointment.

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

James

	Portal	GIPSI	SETEC	Forum	Total
Median	17.0	14.0	16.5	21.0	69.5
Mean	16.8	14.5	15.8	20.3	67.0
Std. Dev.	4.5	4.3	4.5	4.2	14.2

(1) Thinking With Portals

We have a problem because Aperture's privacy promises are in severe tension with its actual conduct. Despite claiming that we know nothing about our users and will strongly preserve their privacy, we have been turning over their communications to the police. This degree of control has important implications for our other legal issues. You will need to decide whether we should protect users' privacy at all costs, or whether we should protect others against our users' misdeeds. I will describe the legal issues that bear on this decision. Either way, we should then bring our conduct and our terms of service into line with the goals we set.

The Aperture Terms of Service and Privacy Policy

Under *ProCD*, Aperture's Terms of Service will be enforceable as a contract if the consumer has (1) notice of the terms, (2) an opportunity to inspect the detailed terms, and (3) an opportunity to back out of the transaction if the detailed terms are unacceptable. Here, the website provides detailed terms, and we will presumably honor refund requests. Notice is more difficult: would an ordinary consumer see the label on the top of the Portal? Unless they are printed in a tiny font or otherwise obscured, it seems likely that a consumer would see the notice while plugging the Portal in.

Thus, Aperture's Terms likely constitute a binding contract. This may not all be to Aperture's benefit; under *JetBlue*, its Privacy Policy may be enforceable against it. In the future, it may be more reliable to use clickwrap or shrinkwrap terms of service.

Sergeant Johnson's Investigation

By keeping copies of the bytes sent to and from users' Portals, Aperture likely violated the Wiretap Act by "intercepting" an "electronic communication."18 U.S.C. § 2511(1)(a). It was an "interception" because Aperture acquired the contents of the users' communications. (It appears that Aperture did this by making a copy of each byte as it was transmitted through the Aperture server.) Under *O'Brien*, the interception would be considered contemporaneous with the original transmission, and therefore would violate the Act.

Aperture may also have violated the Stored Communications Act (SCA) by divulging to Sergeant Johnson the "contents of a communication while in electronic storage," 18 U.S.C. § 2702(a)(1). The users' communications are arguably "in electronic storage" because at the time the Aperture server makes a copy of them, they are in "temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17).

Although both the Wiretap Act and SCA allow such disclosures pursuant to a validly obtained search warrant or court order, no such order was applicable here. Sergeant Johnson's search warrant, it appears, allowed only the search of the suspects' houses; her request to Aperture was "informal." Aperture might be able to argue that it was a "party" to the communications because of the relaying architecture it uses; each half of a Portal connection is directed to Aperture's servers. Aperture probably could not defend itself by pointing to its terms of service or privacy policy, neither of which tells users that Aperture might do something like this.

Thus, I recommend that Aperture immediately stop cooperating with Sergeant Johnson, and refuse to turn over any further customer communications unless required to do so by valid legal process. Whether or not her conduct violates the Fourth Amendment and results in inadmissible evidence is her problem, not ours.

Caroline Atlas's Lawsuit

Aperture is not liable to Caroline Atlas for the posts by Mr. Pee-Body. 47 U.S.C. § 230. (Similarly, Atlas has no legal basis to demand that Aperture cease providing him with service.) Since she has not requested a subpoena from a court, for the moment, we have discretion whether or not to disclose what little we know about Mr. Pee-Body's identity to her. (All we could tell her would be his IP address and the serial number of his Portal.)

It is your decision whether or not to reveal Mr. Pee-Body's identity. On the one hand, based on your "shocked" reaction to Sergeant Johnson's request, you may disapprove of those who use Portals for illegal or harmful purposes. On the other, it will be very unpopular with our privacy-loving customers if it becomes known that Aperture voluntarily breached a user's privacy. In addition, it would open us up to a potential *JetBlue*-style lawsuit for breach of our Privacy Policy. We could attempt to defend by arguing that our Terms of Service prohibit "harassing" conduct, but our case would be stronger if we reserved the right to terminate service or disclose identities for a breach of the Terms. I recommend add those provisions to our Terms of Service.

Black Mesa's Lawsuit

Aperture directly infringes on Black Mesa's public distribution right by transmitting copies of *Enrichment Sphere* to and from Portal users. *London-Sire*. However, we can interpose a strong § 512(a) defense, as the allegedly infringing conduct consists of "transmitting … material through a system or network controlled or operated by or for the service provider" and we qualify as a "service provider" under the stricter definition in § 512(k)(1)(A): the user selects the destination for the content and we don't modify it. That should give us an immunity to copyright infringement claims based on our operation of the Portal service.

Black Mesa may, however, object to our distribution of the Portal device as well as the service. Here, there would be no direct infringement as our role consists only in distributing the device. We could raise a *Sony* defense to a contributory infringement claim, as the Portal has non-infringing uses, like protecting one's privacy. As for a vicarious infringement claim, we do have the right and ability to control the *service* by monitoring user transmissions and cutting off service to specific Portal serial numbers. (We cannot control the *device* once we sell it.) I would argue that we do not have a direct financial benefit from Portal sales, as they are one-time revenue that is not sensitive to future infringing or non-infringing uses; Black Mesa would claim that infringement acts as a "draw" to boost sales. I am not concerned about inducement infringement, as we have not done anything deliberately to encourage the use of the Portal for infringement. Black Mesa could argue that our emphasis on privacy indicates a desire to encourage infringement, but there are many non copyright-related reasons to desire privacy.

(2) Everything's Coming Up Lawsuits

The STRIP Act threatens our members with the loss of a profitable line of business, one that customers are enthusiastic about. The worst case is that we will need to stop offering online strip poker, but I am optimistic that legal challenges and other moves will enable us to avoid that possibility.

First Amendment Issues: Section 1

The STRIP Act's definition of "specified adult activity" resembles the three-prong *Miller* test for obscenity, but deviates from it in multiple ways. First, the first prong requires the application of Utah community standards. Under *Kilbride*, this is unconstitutional; for Internet activity, national community standards must be used. Utah is not in the Ninth Circuit, so *Kilbride* is not binding, but *Ashcroft*, as a Supreme Court case is, and *Kilbride*'s reading of *Ashcroft* is persuasive precedent.

Second, the definition of "sexual conduct," although seemingly based on *Miller*, conclusively defines "patently offensive" to include "partial nudity" and material that "inescapably suggests sexual matters." This extends the boundaries of the Act's prohibitions beyond how the Supreme Court defined obscenity in *Miller*, and therefore prohibits speech protected by the First Amendment.

Third, we can argue that online strip poker has "serious … artistic" value as a game of skill in which the nudity is an integral part of the gameplay. This argument may be a stretch, but we should raise it.

Finally, we can point to the Act's exception of non-commercial and non-credit-card sites to argue that it is also fatally underinclusive. If the state's interest really is in preventing obscenity, it should not care how the obscenity is paid for.

First Amendment Issues: Section 2(b)

We can also object to the Act's felony prohibition on making online strip poker available to minors. I do not think we can seriously argue that it is not harmful to minors, but we can take issue with how the Act tries to shield minors from it. Here, because the STRIP Act will be assessed using strict scrutiny, it must be the least restrictive alternative. We can argue that parental filters are a more effective alternative.

We could argue, based on *Reno*, that the "knowingly" prohibition enables minors to censor protected adult-appropriate speech merely by announcing their presence. However, because our poker games are closed spaces that require age certification to play, it would appear that we could respond to the presence of a self-declared minor simply by ejecting them from the game.

"Recklessly" may be more dangerous to our members; Utah could argue that our age verification techniques are not sufficiently effective. I would like to discuss this angle with some of my contacts who regularly lobby the Utah legislature and executive, to see whether an acceptable compromise could be reached as to which age verification techniques are sufficient.

Dormant Commerce Clause

We can make two arguments under the Dormant Commerce Clause. The first is that the Act regulates extraterritorially by prohibiting online strip poker conducted outside of Utah merely because one of the players or part of the network is in Utah. Utah could respond that our members could use geolocation technologies, as Yahoo! did, to avoid serving Utah residents. However, the Act's definition in § 2(a) would appear to criminalize all online strip poker, because the entire Internet is a network that is "located in Utah … in part."

The second argument is that the blocking requirements in § 4 violate the *Pike* balancing test, much like in *Pappert*. ElectraNet, as a multi-state ISP, is an example of an ISP that would have to sever service to Nevada residents, an impermissible burden on interstate commerce. Using the most common forms of blocking, other websites would also be blocked, again an impermissible burden.

Jurisdiction

I have some concerns about the scope of Utah's jurisdiction over out-of-state GIPSI members. However, Mazeppa was arrested while physically in Utah, as were Merman and Lee. It is possible to imagine a *Voyeur Dorm*-style defense that the online strip poker is only "online" for jurisdictional purposes, because it is carried out entirely through webcams with no physical presence. However, unlike the zoning statue in *Voyeur Dorm*, the STRIP Act is aimed at the harms caused by online strip poker.

Process Concerns

Under *Kremen*, domain names are property that could validly be seized. One wonders where they are, however, for jurisdictional purposes. It is hard to see how PokerHavoc.com is property located in Utah. There are also serious due process concerns with the way the Act is being enforced, as in the recent ICE seizures of sports broadcasting websites before the Super Bowl. RoseColoredSlots's plight illustrates that the Attorney General's list of online strip poker sites is error-prone, and that innocent sites are being swept up in the dragnet.

Advice

I recommend that, for the time being, GIPSI members comply with the act by not offering online strip poker, by redesigning the game so that stripping is not a "prize" for winning (e.g. players could simply remove clothing in they order they play), or by not taking payment with credit cards. I will try to explain the Act's constitutional infirmities to the Utah legislature and Attorney General. If that fails, I can file a lawsuit to invalidate the STRIP Act as unconstitutional and enjoin its enforcement. We could also intervene in the cases of Mazeppa, Merman, and Lee, to help with their defense. Ultimately, since such a profitable venture is at stake, I recommend that our members pool together to fund a legal challenge to the Act, which is likely to succeed.

(3) Too Many Secret Keys

Personal Jurisdiction

All of Playtronics' operations are in New York, so it is subject to jurisdiction there. Because she lives and works in New York, Emery is subject to jurisdiction there. Crease's only relevant contact with New York is that he released his software to generate keys for Passport, which was produced by a New York company. (The server does not suffice as a contact because the claims against him have nothing to do with the server itself and he was unaware of its location, as in the *Too Damn High* problem.) This might count as an intent to direct activity to New York, but *Boschetto* might also treat this as a fortuitous, isolated contact with no specific focus on New York. As for Rhyzkov, all he did was maintain a bulletin board accessible from anywhere in the world. He never dealt specifically with anyone in New York, and his role with regard to Emery's post was completely passive. Jurisdiction over him is unlikely

Bishop's Lawsuit

Bishop may sue Playtronics for infringing his copyright with Passport, which is a modified version of SETEC because it "incorporates" SETEC code. Although the GPL grants permission to "copy" and "modify" the licensed software, when Playtronics decided to distribute Passport), it triggered additional obligations. Clause 2(b) requires that the modified version be relicensed under the GPL, but the Passport terms of service are much more restrictive than the GPL. Clause 3 requires that Playtronics make the source code of the modified version available, which it apparently has not done, as it prohibits reverse engineering. Further, it is unclear whether Playtronics has provided the attribution required by clause 2(a). These violations of the GPL are enforceable by Bishop as copyright infringement, as they are conditions of the license, not covenants. *Jacobson v. Katzer*,

Emery is fully protected by the GPL's grant of permission to "copy" and "distribute" the software. She has done nothing to infringe Bishop's copyright in SETEC. When she posted her findings, even if she posted excerpts from the SETEC code, she had not modified the code, and therefore did not trigger any further obligations. Indeed, Bishop should be grateful to Emery for exposing Playtronics' violation of the GPL; it does not make sense for him to sue her.

Bishop also has no case against Crease, who appears to have fully complied with his obligations under the GPL. He made source code available and relicensed his modified version under the GPL. (It is possible to assume that Crease failed to provide proper attribution, but the opposite assumption is just as reasonable.) The GPL imposes no obligation to provide object code.

Playtronics' Lawsuit

Playtronics will first assert that Emery violated its terms of service by reverse engineering the software. It will claim that she as acted "contrary to the spirit in which it is made available" and attempt to charge her 25 cents per song, for a total of $2,500. Emery has no serious defense under *ProCD* and *Specht*; she clicked "I agree" to valid clickwrap. However, she may claim under *Bragg* that the terms are unconscionable. They are procedurally unconscionable as a contract of

adhesion. Substantively, charging a "restocking fee" for a digital file is nonsensical, and Playtronics' "sole and unappealable discretion" is a one-sided term like those struck down in *Bragg*.

Next, Playtronics will claim that Emery violated its rights under Section 1201 of the DMCA. Passport is a "technological measure" that "effectively controls access" to the music because it requires the application of a secret key to gain access to the work. Emery, however, can correctly respond that she has not actually violated § 1201(a)(1), because she herself never circumvented Passport. She did not "descramble …, decrypt … , avoid, bypass, remove, deactivate, or impair" Passport or any of the tracks.

Playtronics, as a fallback, will claim that she violated § 1201(a)(2) by trafficking in an anti-circumvention technology. Emery's response here would be that she has shared knowledge about Passport with the public, rather than providing a technology that anyone could actually use. In light of the DeCSS controversy over what counts as such a technology, this is a difficult question; it will help Emery's case that she was exposing Playtronics' own wrongdoing.

Since there is no indication that anyone has actually decrypted any tracks, Playtronics (or rather, the copyright owners in the music) have no case of primary copyright infringement against anyone based on the songs, and therefore also no case of secondary infringement. Playtronics might, however, use its terms of service and the fact that Emery downloaded Passport to argue that the terms were conditions under *Jacobsen* and therefore she became a copyright infringer when she violated them.

Rhyzkov will be fully protected by Section 512(c), unless and until Playtronics issues him a DMCA takedown notice. (Playtronics might respond that, per *Remeirdes*, DMCA liability is not copyright infringement and Section 512 therefore does not provide immunity to it.) Even if he is not, then he will be violating Playtronics' rights only if Emery's posting violated them, so he can raise all of the defenses she could raise to DMCA liability.

Playtronics cannot use its terms of service against Crease, as he never visited its site to agree to them. Nor can it raise a copyright claim of any sort; he never downloaded Passport. A 1201(a) claim against him will also fail; like Emery, he did not himself circumvent anything. A 1201(b) claim may be more viable; his program is arguably a technology intended primarily to circumvent Passport protection and with no purpose other than doing so. (That he called it Passport *Forger* will not help him.) He can raise a similar defense to Emery's, arguing that his program by itself is useless, as he provided only source code, but by his own admission, a worthy program could compile it into an executable object code version.

Playtronics may also assert trademark infringement against Crease, based on his use of the trademark PASSPORT in his program name, the passportforger.com domain name, and his metatags. The domain name also gives rise to an ACPA claim. Crease's defense will be that his use of the name does not cause confusion; consumers will understand that his product is not Passport itself but a program that creates Passport keys. This argument is persuasive under *Taubman*, especially since his use is noncommercial.