Internet Law

Professor Grimmelmann

Final Exam - Spring 2011

Take-Home and Open Book

This exam consists of THREE equally weighted questions. The exam counts for 75% of your grade in the course.

This exam will be available on Wednesday, May 4. You must upload your answer via the Exam4 web site by 5:00 PM on Tuesday, May 16.

Type your answers in 12 point Times or Times New Roman, double-spaced, using 8.5"x11" paper, with one-inch margins and numbered pages. Put your exam number on each page. DO NOT PUT YOUR NAME ANYWHERE ON THE EXAM.

There is a page limit of FOUR pages per question.

This is an open-book exam. You may use any materials that you wish to answer the questions, though you need not consult any sources other than those we used for class. You may not discuss this exam or your answers with anyone under any circumstances until after the end of exam period. **Your work must be exclusively your own**.

I will not answer questions about the course after the start of exam period.

Please pay attention to the specific questions being asked and to the roles the questions place you in. Support your answers with detailed analysis, reference to specific statutes and cases as appropriate, and explanations of how you applied the law to the facts. Simple citations (e.g. "Zeran.") are appreciated but not required. Basic headers to organize the different parts of your answer are also a good idea.

If anything about a question is ambiguous, say what you think it means, and answer it accordingly. If you need to assume additional facts, say what those facts are and how they affected your answer. No reasonable resolution of an ambiguity will be penalized.

This exam has **FIVE pages total**, including this cover sheet.

GOOD LUCK!

Question 1: Thinking with Portals

You are outside counsel to Aperture Industrial. It sells a $499 device called the Portal, which it promotes as a "revolutionary new way to protect your privacy online." The Portal is a sealed white box that plugs into a USB port on your computer and has an Ethernet jack to connect a network cable. Once set up, the Portal contacts an Aperture server at IP address 114.12.59.4 and relays all of your computer's Internet traffic through it. Whenever a Portal-equipped computer needs to send an IP packet to some other computer X on the Internet, the Portal sends the packet to the Aperture server at 114.12.59.4 instead. That server then forwards the packet to computer X, giving 114.12.59.4 as the return address. If X sends any IP packets back in return, the Aperture server then forwards them to the Portal. The result is that computer X believes it's communicating with the computer at 114.12.59.4. It never learns the user's IP address, which only Aperture knows. Aperture provides this service for free for the lifetime of the Portal. Each Portal has a unique serial number, which it uses to authenticate itself to Aperture's servers. This way, Aperture has no billing relationship with users and doesn't need to know their names, real-world address, credit card numbers, or any identifying information other than IP address.

Gladys Wheatley, Aperture's CEO, has asked for your advice on a number of matters:

- Aperture's Privacy Policy, posted on its website, states, "Aperture is committed to protecting your privacy and will never do anything to compromise it. In case you still don't trust us, consider this: we don't even know who you are!" Its Terms of Service, also posted on its website, require users not to use the Portal for any purposes that are "obscene, harassing, infringing, or otherwise in violation of law." There is no signup process, but printed on the top of each Portal is the text, "Use of this device constitutes acceptance of our Terms of Service and Privacy Policy. See apertureindustrial.com for details."
- Sergeant Chell Johnson, of the Marquette, Michigan police department, emailed Aperture in February of 2010, informally requesting help in investigating an ongoing methamphetamine distribution operation; Sergeant Johnson believed that the criminals were using Portals to communicate. Wheatley, shocked, gladly agreed to help. Johnson provided a list of Portal serial numbers (determined by secretly executing search warrants on the suspects' houses and physically examining their devices). Since then, Aperture has been keeping copies of every byte sent to or from these Portals. Once a month, it turns the complete logs over to Johnson.
- Caroline Atlas, a 17-year-old from Indiana, has been viciously attacked by a long series of blog comments posted by someone using the alias "Mr. Pee-Body," claiming that she has attempted to poison her classmates using deadly neurotoxin. Atlas has identified the IP address from which Mr. Pee-Body's comments as 114.12.59.4. She has filed a John Doe suit against Mr. Pee-Body; her complaint also names Aperture as a defendant. She is demanding that Aperture (a) identify Mr. Pee-Body to her attorney, (b) terminate service to him, and (c) pay damages for the harm his comments have done to her reputation.
- It appears that a large number of Portal users upload and download movies. Some of them are independent filmmakers distributing their own works; many, if not most, are copying the latest Hollywood blockbusters without permission. Last week, Black Mesa Studios filed suit against Aperture, claiming direct, contributory, vicarious, and inducing infringement for the actions of Portal users in uploading and downloading Black Mesa's copyrighted movie, "Enrichment Sphere."

Wheatley has asked you advise Aperture on the legal issues these developments raise, and to suggest what it should do in response. Write a memo with your advice.

Question 2: Everything's Coming Up Lawsuits

You are the general counsel for the Gaming and Interactive Products Software Institute (GIPSI), a trade group for companies in the gambling industry. Recently, a number of gambling websites have begun to profitably offer what they describe as "online strip poker." Players, who must register with a major credit card and click a box affirming that they are over 18, must have webcams, and, yes, are required to remove an article of clothing each time they bet on a hand and lose. It is a well-known secret that at least one player at each table is a highly attractive shill employed by the website offering the game. (The shills, however, are frequently expert poker players, so their attractiveness alone is not the only draw, and they regularly outplay many or all of the others at their table.) The websites have discovered that enough players become careless as the clothes start to come off that the games are quite profitable.

The state of Utah recently passed the Stopping The Reign of Immoral Poker (STRIP) Act, which is targeted at sites offering online strip poker. Section 1(a) of the Act defines "online strip poker" as "any game of chance and/or skill, offered via the Internet or other electronic computer network, the prize or reward for which is specified adult activity." Section 1(e) defines "specified adult activity" as:

> "any activity that
>
> (1) the average person, applying the contemporary community standards of the state of Utah, would find that the work, taken as a whole, appeals to the prurient interest;
>
> (2) depicts or describes in a patently offensive way sexual conduct of any sort, including without restriction full or partial nudity, actual or simulated sexual intercourse, or that inescapably suggests sexual matters to a person of ordinary morals;
>
> (3) and lacks serious literary, artistic, political, or scientific value."

Section 2(a) makes it a civil and criminal offense to offer online strip poker "from Utah, to Utah residents, or via a network or computer located in Utah in whole or part." Section 2(b) makes that criminal offense a felony if the defendant "knowingly or recklessly offers online strip poker to a minor." Section 3 permits the state attorney general to seize any "premises, facility, computer, domain name, or other property used in the commission of the violation of the Act." Section 4 requires ISPs serving Utah customers to block access to all online strip poker. Section 5 of the Act exempts sites offering online strip poker from the restrictions of the Act if they do not charge a fee to participate or are paid through means other than a credit card.

A month ago, the Utah attorney general sent a letter to ElectraNet, an ISP serving customers in Utah and Nevada, listing 106 websites that it described as offering online strip poker. You have received a copy of the list, and most of the websites are operated by members of GIPSI. You have checked with some, which confirm that they offer online strip poker, although one site on the list, RoseColoredSlots, denies that it does so.

Last week, state police arrested Herbert Mazeppa, the owner and president of PokerHavoc.com, as he was changing planes in the Salt Lake City Airport. PokerHavoc's offices and servers are in

Tulsa, Oklahoma. The indictment charged Mazeppa with violating the STRIP Act, and alleged that PokerHavoc had supplied online strip poker services to six Utah residents on a total of ten occasions. Two days later, they raided the Provo, Utah offices of EntertainU.com, another website offering online strip poker, and arrested two of its employees: the poker player Louise Lee and the sysadmin Tessie Merman. The attorney general indicated at a press conference that he plans to move to seize any of PokerHavoc's and EntertainU's assets he can reach as soon as possible.

You have been asked to prepare a legal strategy for responding to the STRIP Act. Draw up a strategy memo describing the legal risks the Act poses to your members, possible theories for challenging it in court, and your proposed strategy for how the association should proceed.[1]

Question 3: Too Many Secret Keys

Cosmo Bishop is a programmer who lives and works in Maryland. He developed the popular SETEC encryption program. It provides a fast and flexible set of basic operations for encrypting and decrypting material and other common operations. He released it under the GNU GPL version 2, placing both source and object code versions on his website.

Playtronics is a music company, all of whose operations are located in New York. It offers free "downloads" of any song the user wants. The gimmick is that each download comes in encrypted form, together with a key good for one listen only. Its Passport music player will use the key to play the song for the user once, after which it deletes the key. The user can then go back to the Playtronics site and, if she wishes, pay 99 cents for a permanent key that "unlocks" the song for an unlimited umber of plays. The idea is that since only the (much smaller) key needs to be downloaded the second time, rather than the full song, users will be more willing to buy the song for instant gratification. The terms of service on Playtronics.com, to which the user must click "I agree" before downloading any tracks, read, in part:

> The Passport software and all Content [i.e. music available through the site] are licensed, not sold. They are made available for personal, noncommercial use only. You may not reverse engineer the software or attempt to determine its functionality. In the event that your use of the software is deemed contrary to the spirit in which it is made available, you agree to pay a restocking fee of 25 cents per track downloaded, to be charged in Playtronics' sole and unappealable discretion.

Liz Emery is a music fan and programmer who works out of her home in New York. She downloaded a few songs using Passport and then paid to unlock them. Out of curiosity, she started trying to figure out how Passport encrypted its songs. She downloaded 10,000 songs from Passport over the course of several days and started analyzing them. By noticing a certain unusual pattern in the encrypted version of the songs, she realized that Passport was based on SETEC. She spent several weeks studying how Passport worked, and was able to confirm that it incorporated substantial portions of SETEC code.

Emery posted her findings about the origin of Passport to JanekTek, a discussion board for programmers interested in encryption technology. JanekTek is hosted on a computer in the Russian Federation; its administrator, Werner Rhyzkov, lives in Moscow.

---

[1] [You should ignore any issues relating to the legality of online gambling, which we did not cover in this course. -JG]

After reading Emery's post, another JanekTek user, Darren Crease, realized that he could easily generate decryption keys for Passport tracks using functions built into SETEC. He wrote a short program, incorporating code from SETEC, that would generate a decryption key for any Passport file. Being arrogant about his technical skills, Crease never bothered to test whether his program worked—indeed, he never looked at the Passport software, visited the Playtronics site, or signed up for a Passport account.

Crease posted his new program, which he called Passport Forger, at passportforger.com, and put the words "passport, passport forger, playtronics, decryption, passport decrypter, passport keys, passport sucks crease rules" in the meta tags of his site. He posted only the source code, explaining that anyone who couldn't compile the source code into executable object code wasn't worthy of his time. He released all of his modifications under the GNU GPL version 2. Crease lives in California and he used BlackBoxes.com, a San Francisco-based hosting service, for the passportforger.com site. (Unbeknownst to Crease, however, BlackBoxes hosted his website from its New York City data center.)

That was about when the lawsuits started. Bishop sued Playtronics, Emery, and Crease in the federal District Court for the Southern District of New York. Playtronics filed its own suit, also in the Southern District, against Emery, Rhyzkov, and Crease.

You are clerking for Senior Judge Carl Abbott, who has been assigned the cases. He has asked you for your initial advice on the legal issues it raises, so he can start planning for the case management conference. Write a memo sketching out the various parties' claims against each other and potential defenses for the judge, and giving a preliminary assessment of which of them are likely to succeed.