Final Examination Memorandum
Internet Law
Spring 2016
Professor Grimmelmann

I graded each question using a checklist, giving a point for each item (e.g., "DEI is not a direct infringer.") you dealt with appropriately. Ten percent of the credit in each each question was reserved for organization and writing style. I gave partial credit for partially correct analyses; I gave bonus points for creative thinking, particularly nuanced legal analyses, and good use of facts.

Sample answers to the three questions are below. They 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 have further questions after comparing your essays to the model answers, or would like to discuss the course or anything else, please email me and we'll set up a time to talk.

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

James

Question 1: Encryptinator

Logs

DEI should not voluntarily disclose to the FBI the logfiles from its server at encryptinator.com. Doing so might be a violation of 18 U.S.C. § 2702(a)(3), which states, "a provider of … electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service … to any governmental entity." The FBI is a governmental entity, and the logs identifying Encryptinators and when they logged in are records pertaining to customers. (They include several of the items available under §§ 2703(c) and (d), including connection records, instrument numbers, and network addresses.)

The one subtlety is that DEI might not be considered a provider of electronic communications *service* as defined in 18 USC § 2510. It sells devices, and all communications pass between those devices directly, rather than by way of DEI's servers. But DEI still provides its users the "ability" to send and receive electronic communications by providing the server that enables Encryptinators to locate one another, so it probably is a provider covered by § 2702(a)(3).

None of the exceptions in § 2702(c) applies. Users have not consented to disclosure; indeed, DEI's terms of service state that information will be shared only "as *required* by law" (emphasis added). Disclosure is not necessary to provide the service or to protect DEI's rights; nor is there an "emergency involving danger of death or serious physical injury."

Agent Perry will be able to compel disclosure of the logs if she returns with a properly authorized order under § 2703(d). But to obtain such an order, she must "offer[] specific and articulable facts showing that there are reasonable grounds to believe" that the records are relevant. That is her burden, not DEI's. DEI should consider objecting to the scope of the request; it may be that the complete logs would be "unusually voluminous" and that the specific and articulable facts show only that some subset of the logs are relevant to the ongoing investigation.

There is no Fourth Amendment problem with compelled disclosure of the logs. Like the records of phone numbers dialed in *Smith v. Maryland*, they are a form of addressing metadata that are shared with a communications provider. As such, the third-party doctrine applies to them.

Cryptix

The FBI's request for a modified version of Cryptix is problematic for many reasons. First and foremost, it would cause a serious violation of the Wiretap Act. The communications sent between Encryptinators are electronic communications, and the modified version of Cryptix would engage in the "interception" of those communications in violation of § 2511(1)(a). As in *O'Brien*, retaining an unauthorized copy of a communication and making that copy available to a third party would constitute prohibited interception.

As above, there are no applicable exceptions in § 2511(2)(a)(i). The parties have not consented; DEI does not need to intercept messages sent between Encryptinators as a

"necessary incident" of its service or to protect its rights; and encrypted communications are definitely not "readily accessible to the general public."

This time, Agent Perry's threat to obtain a (d) order is toothless. For one thing, a (d) order can only be used to obtain the *contents* of electronic communications – which is what the unencrypted message are – when they have been in electronic storage for more than 180 days. *Id.* §§ 2703(a), (b). Messages being sent between Encryptinators in real time have not been in electronic storage more than 180 days, if they are in electronic storage at all.

Even if the Stored Communications Act did apply, its use here (to obtain the contents of electronic messages) would be in violation of the Fourth Amendment. *Warshak*. That Encryptinator users have a reasonable expectation of privacy is confirmed by the repeated promises in the terms of a that all communications are secure and no information will ever be shared. Agent Perry will need to obtain a search warrant and to meet the heightened protections imposed by the Wiretap Act when she does.

In addition, Agent Perry's demand that DEI itself create the modified version of Cryptix is unlawful. She has identified no legal basis for the demand – and certainly not § 2703, which requires only disclosure of communications and records possessed by a service provider. The All Writs Act might work, but its applicability is currently being litigated in cases involving Apple. Like Apple, DEI could assert that it has a First Amendment right not to be forced to "speak" by creating the modified software, although whether *Bernstein* actually reaches this far is subject to dispute. Finally, DEI might violate the Computer Fraud and Abuse Act by installing this "update" on Encryptinators without the consent of their owners. Encryptinators are protected computers; installing the modified version of Cryptix would be an access to them. The only argument that owners have authorized this access is the clause in the terms of service that DEI may "update" the software "to add features, fix bugs, and make other improvements." Breaking the encryption so that communications are turned over to third parties is probably not covered by this form of "consent."

Jeremy X

Although the child pornography being shared through the Encryptinators is information provided by third parties, section 230 will not protect DEI here. *See* 47 U.S.C. § 230(e)(1) (providing that section 230 does not apply to violations of federal criminal laws, including laws "relating to obscenity" and "relating to sexual exploitation of children"). That said, DEI can voluntarily attempt to limit the availability of this material without being concerned about legal risk; section 230(c)(2) provides that it will be immune for good-faith attempts to restrict access.

Unfortunately, there is simply not much that DEI can do here without breaking the most basic feature of its product: strong encryption. Because the secret keys are known only to the Encryptinators in a pair, not even DEI can inspect the messages or identify when they contain child pornography. (The messages themselves do not even pass through DEI's servers at any point.) Nor can it tell which Encryptinators are being used to exchange child pornography, so it would have no way of knowing which users to deny service to. DEI could update its software to weaken the encryption or to filter message

before they are encrypted, but such a change would seriously weaken its ability to claim that it provides reliably secure encryption. If DEI did it for Jeremy X, who would be next?

The MPAA

DEI is not a direct infringer. It never reproduces, distributes, performs, or displays any copyrighted works. Encryptinator users may reproduce and distribute works – and perhaps even perform them if they sing into the microphones – but that makes the users the direct infringers, not DEI.

DEI is not a secondary infringer, either. It is not a vicarious infringer because there is no indication that the ability to share copyrighted works acts as a "draw" when selling Encryptinators, and it is utterly without the ability to control how Encryptinators are used once they are sold. It is not a contributory infringer because it has only generalized knowledge that Encryptinators might be used to infringe, so that even if it makes a material contribution to the infringement by selling Encryptinators, it has a *Sony* defense since they are capable of exchanging all kinds of other messages securely. And it is not an inducing infringer because it has done nothing to promote the use of Encryptinators for infringement. DEI does not need to do anything to help out the MPAA, and it could not, for reasons discussed above.

Terms of Service

The terms of service are probably binding as a contract. They provide clear notice to users that there are terms and, as in *ProCD*, they treat continued use as acceptance. One potential problem is that the terms do not block access to the Encryptinator's functionality until the user agrees to them for the first time, so continued use might not sufficiently manifest acceptance.

The strong promises of secure encryption and against data sharing open up DEI to potential liability if it cooperates with Agent Perry, Jeremy X, or the MPAA. "As required by law" gives DEI the room it needs to comply with binding court orders, but none of them have shown up with such an order yet. Breaching these promises by sharing user data without a court order might not be sufficient to give any Encryptinator owners standing to sue, but as in *Snapchat* it could be treated as a deceptive practice leading to FTC enforcement.

Conclusion

Because DEI's business depends on giving its customers unbreakable encryption, it should strongly resist any attempt to compromise that protection. Even aside from the legal ramifications, the bad publicity could be fatal to its business.

Question 2: Bust My Brother

Torts

Candace's vow to "bust my brother" and her assertion that she would"[k]ick [his] ass" are probably not actionable as threats. The former is too general and the latter is too hyperbolic to make a reasonable listener think that they were immediate and unequivocal. But her insinuation that someone might disable the brakes on his car may be unprotected by the First Amendment (and hence sufficient to ground an intentional infliction of emotional distress claim). It is a specific threat about a particular means of physical harm, and her appeals to other users suggest she may be trying to recruit one of them to disable his brakes.

Candace's request to "Tell Phineas what you really thing [sic] of him" is probably not actionable. Under *Marquan M*, speech that embarrasses or annoys but not more is protected by the First Amendment, even if uttered with bad motives. Encouraging others to do the same is similarly protected, at least when the worst Phineas has experienced as a result is insulting emails. *Cf. Hamidi* (holding that spam is not sufficient to support a claim for trespass to chattels unless it damages or impairs a computer).

The statements on phineasflynn.com about the rollercoaster state a claim for defamation. If they are untrue – as Phineas asserts and therefore must be taken as given on a motion to dismiss – then they are false and likely to cause economic harm to his amusement park. The statement about the two deaths, if it is as unsubstantiated as Phineas claims, is so without foundation that it would appear to support an inference of reckless disregard for the truth, and thus show actual malice.

The photograph on the coffee mug is probably not actionable as defamation; the scars and warts might be seen as a kind of visual hyperbole. Phineas would need to show that a reasonable person would think that he actually looked that way. He might be able to argue that selling coffee mugs with the photograph on them violates his right of publicity. But the mugs are not really trying to profit off the value of his image; quite the opposite, they are a form of criticism designed to challenge that value.

Domain Name

"Phineas Flynn" is not a trademark; there is nothing to indicate that Phineas has used his name on goods or services to indicate the source of goods. It's just his name. As as result, he cannot sue for trademark infringement, cannot bring an ACPA action, and cannot bring a UDRP proceeding on the basis of the use of his name on the phineasflynn.com domain name. To be sure, the use of a fictitious name when registering the domain is a factor tending to show bad faith, *see,* 15 U.S.C. § 1125(d)(1)(B)(i)(VII), some courts have treated the use of a domain name without a "sucks" or similar suffix as preventing a parody or criticism defense, *see, e.g. Doughney*, and Tjinder is making what some courts would treat as a commercial use by selling coffee mugs, *see, e.g., Taubman*. But without trademark rights in the first place, Phineas cannot even reach that stage of the analysis. The UDRP arbitrator was wrong to award Phineas the domain name; Judge Hirano should dismiss his trademark causes of action.

A section 8131 claim should also fail. Phineas does have the necessary rights in his own name, but here there is no "specific intent to profit from such name *by selling the*

domain name for financial gain to that person or any third party" (emphasis added). Since Tjinder is using the domain name simply to mock Phineas and to sell other products, rather than to sell the domain name itself, he is safe.

Motion to Intervene

Tjinder's motion to intervene should be granted. Phineas's subpoena to Ferb.it gives Tjinder a concrete stake in the outcome of *Flynn v. Flynn*; he must be permitted to appear at least to move to quash the subpoena. Once he is already before the court and given that several of Phineas's claims are directed against him (albeit under the theory that Tjinder is Candace), it makes sense to allow him to litigate his rights in the domain name in the same case, rather than forcing him to file a new declaratory judgment action.

Motion to Quash

Tjinder's motion to quash the subpoena should be denied. For purposes of Phineas's defamation claim, Tjinder's identity is centrally needed. Otherwise, Phineas cannot be sure he has named and served the proper defendant. Phineas has produced sufficient evidence to meet the "concrete showing" standard: he has identified the allegedly false and defamatory statements and provided competent evidence (his own declaration) that those statements are indeed false. Ferb.it is not the only source that might have information on Tjinder's identity (there is also the coffee mug vendor), but it is better than any of the alternatives.

Choice of Law

Candace's argument that United States law cannot apply to her conduct is incorrect. *See Gutnick, Mahfouz.* As discussed above, Phineas has stated at least one viable claim under United States law, so there is no inherent obstacle to applying that law to her.

Personal Jurisdiction

Candace's motion to dismiss for lack of personal jurisdiction should be granted. She is not a domiciliary of Danville, she was not served while in Danville, she has no property in Danville, and she has not consented to the court's jurisdiction. That leaves only specific jurisdiction. But Phineas has pleaded no facts tying any of the conduct at issue to Danville in any way. He has not pleaded that he is a resident of Danville, that The Old Abandoned Amusement Park is in Danville, or that Norm.com or its users are in Danville. The case apparently has no contacts with Danville other than that Phineas filed suit here.

If we assume that Phineas, the amusement park, Norm.com, and its users are all in Danville, personal jurisdiction over Candace seems likely. *Burdick* holds that posting defamatory statements about a person while knowing they reside in the forum does not by itself create personal jurisdiction. But Candace's attempts to threaten Phineas and her recruitment of others to harass him are both conduct specifically intended to harm Phineas, and thus represent a more substantial basis for asserting personal jurisdiction over her. Reaching out to other users to invite them to harass Phineas creates relevant contacts with all of those users; so does selling coffee mugs in a way targeted at Danville residents.

As an aside, there is no problem asserting personal jurisdiction over Tjinder. He has submitted to the court's jurisdiction in this matter by moving to intervene.

Question 3: I Meant It When I Said Section 230 Would Be on the Final

(c) ***Protection for "Good Samaritan" blocking and screening of offensive material***

(1) ***Treatment of publisher or speaker***

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.

(2) ***Civil liability***

No provider or user of an interactive computer service shall be held liable on account of –

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

Section 230 prevents intermediaries like Comcast, Facebook, and Google from being held liable for content posted by users. In *Zeran v. AOL*, for example, AOL was held not liable for the defamatory statements posted by "Ken ZZ03" about Ken Zeran, even after Zeran complained about those posts to AOL.

I promise that I will always remember to ask whether Section 230 applies if I am working on a case involving user-generated content.