Internet Law

Professor Grimmelmann

Final Exam - Spring 2014

I graded each essay question using a checklist, giving a point for each item (e.g., "Even if Clevinger's lawsuit is dismissed for lack of personal jurisdiction, he could refile in California, where she is domiciled.") 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

(1) Rowboat

Substantive Liability

You face liability under the Computer Fraud and Abuse Act and potentially under state computer misuse statutes. Clevinger's laptop is a "protected computer" because he used it in interstate commerce by transporting it across state lines and downloading programs from other states. You "accessed" it by causing the auto-updater to install your patches. Clevinger gave you authorization to install Rowboat when he downloaded it initially, but that authorization could not have extended to the updates, because you never gave notice in any form that you would transmit updates from your server to computers running Rowboat. The February update caused "damage" to Clevinger's computer by deleting his novel and jazz recordings. If those recordings cost money to replace, or if Clevinger has spent money to investigate and try to recover the lost files, then the update also caused "loss." Thus, it is likely that you violated § 1030(a)(5)(B) or (C) of the CFAA. I am concerned that a jury might find that you acted "recklessly" (under (B)) because you were aware of a risk that a program that modifies files might modify them incorrectly. I am also concerned that Clevinger may have an easy time meeting the $5,000 loss threshold in § 1030(g) to bring a civil suit. The April update intentionally caused "damage' because you programmed it specifically to delete files, so it is a clear violation of § 1030(a)(5)(B). But you may be able to argue that the removal of the log files, standing alone, does not satisfy the $5,000 loss threshold. In addition to the risk you face of a civil suit, it is possible that you might be criminally prosecuted for violating the CFAA. I am less concerned about that risk, however, as your actions were on the whole well-intentioned and prosecutors would prefer to direct their resources against deliberate wrongdoers.

You also potentially face civil liability under a negligence theory for programming and transmitting a defective upgrade that caused harm to Clevinger (and perhaps other users).[1] Unlike in *Rosenberg v. Harwood*, a victim would not have known that using your software created a risk of the harm that ensued and would not have been as able to guard against it. The loss of user data was a foreseeable risk of a coding error on your part, and it is arguable that you had a duty to guard against it.

Finally, I am worried that your deletion of the log files might be seen as spoliation of evidence and subject you to litigation sanctions. Please assure me that you will not send out any further automatic updates without checking with me first.

Liability Waivers

You can argue that the MIT License's all-caps warranty exclusion clause insulates you from civil liability. Because the notice of the license is presented immediately above the download link, it appears to satisfy the *Specht* test of putting a reasonably prudent offeree on notice that the software is supplied subject to a license. I think this will suffice as a disclaimer of any promise that the software would work. I do not think, however, that it suffices to waive liability for non-promissory theories (e.g., by constituting "authorization" under the CFAA) unless users were aware that by downloading the software they were accepting the license. The text on the download page did not suggest that downloading and using the software constituted acceptance: like the license itself, it did not purport to be a contract.

The pop-up that you installed in the April update is probably also not effective to waive your liability. It clearly passes the *Specht* test because the user must click to agree at a time when the liability waiver has been clearly presented. But it may fail the third prong of the *ProCD*

[1] We did not discuss trespass to chattels in this course, but I accepted a trespass to chattels argument in place of the negligence one.

standard that there must be a "right to return." True, Rowboat is free. But presenting the terms in a way that leaves the user no option other than to click where ordered may not count as a meaningful manifestation of assent. Users who have other documents open may not be in a position to restart their computers, even if they understand that doing so is a possible alternative to clicking. The language of the release, too, may not be effective retroactively as to claims for damage that has already occurred. All in all, I would not count on the license or pop-up to protect you.

Jurisdiction

Under the New York long-arm statute, you may well have caused injury in the state. The place of injury for Clevinger's loss of data is probably best described as the place where the data is stored. That could be either New Jersey or New York, depending on where the laptop was when Rowboat deleted the files. If the place of injury is treated as the place of injury to the data's owner, that might depend on whether Clevinger's novel and jazz recordings were used for home purposes (New Jersey domicile) or work purposes (New York). I would not say that you are out of the woods here without more facts. If there was indeed injury in New York, then you probably should have reasonably expected that it would occur there as a result of your actions outside the state, as a bug in Rowboat could cause harm in any state. But fortunately, you do not derive substantial revenue from Rowboat, which is provided for free, and thus do not satisfy the final prong of the statute. You are not subject to personal jurisdiction in New York.

That said, I should note that the exercise of personal jurisdiction over you in many states where Rowboat deleted data would probably satisfy the due process minimum contacts inquiry. You did not direct your actions specifically into any state when you made the program available for download, but with 10,000 users having lost data, there are likely states where you have

hundreds of victims. Under those circumstances—and particularly since you deliberately pushed the buggy February update and the log-deleting April update out to all of your users—courts might consider that you specifically reached out to every state where you have users.

In the long run, fighting personal jurisdiction is not likely to be a winning strategy. Clevinger or another user could simply refile in California, where you are domiciled.

Advice

Consider settling quickly and quietly with Clevinger, lest other users take notice and sue you also. If you settle, ask for a confidentiality clause. A public apology to your users for the bug, and announcing that you've already deployed a patch to fix it, is also likely to build good will and reduce the likelihood of being sued.

Going forward, you should consider making a stronger click-through process either on download or on installation to make users consent to a clearer liability waiver. You might also consider adding arbitration, venue, and choice-of-law clauses, to reduce the expense of any potential suits that users might file, and consider a general class-action waiver.

Finally, you should give users better notice of the auto-update feature that cause all this trouble in the first place, and give them the option to disable it if they wish.

(2) Aardvark

Jurisdiction

Aardvark is located in Virginia and subject to the jurisdiction of the Virginia courts. Unless the § 2703(d) order is itself illegal under state or federal law, Aardvark must comply.

Fourth Amendment

Users' posts to Aardvark are protected by the Fourth Amendment. Users have expressed a subjective expectation of privacy by choosing to use Aardvark with its encryption features. That expectation is probably one that would be considered reasonable by society under the reasoning of *Warshak*. To be sure, forum posts are intended to be read by several other users, perhaps many other users. But the government is not obtaining the posts from those users and there is no indication that the circle of users with access to the Our Name Is Mudd forum is so large as to suggest that they should expect that the posts will be publicly shared. Thus, to the extent that the § 2703(d) order demands posts to Aardvark, it violates the Fourth Amendment.[2]

Whether the metadata requested in the § 2703(d) order (dates, times, sizes, and IP addresses) are protected by the Fourth Amendment is a harder question. By analogy to *Smith v. Maryland*, the fact of a communication would appear to be subject to the third-party doctrine, and thus unprotected. There is a colorable but probably unsuccessful argument under *Klayman v. Obama* that the scale of the collection here would change the *Smith* analysis; but not only have other courts disagreed with *Klayman* but the posts to one discussion site fall far short of the records of every American's phone calls.

[2] We did not discuss in this course the question of who has standing to raise this argument.

Stored Communications Act

There is also a statutory problem with the § 2703(d) order. The Stored Communications Act allows access to an "electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less," only with a search warrant. The § 2703(d) order, which requires only a showing of specific and articulable facts, is not a search warrant, which requires a showing of probable cause. Thus, the order is facially invalid as to the messages on the Our Name is Mudd forum that have been stored for 180 days or less. It is also facially invalid as to the new messages from user Yossarian22, which not only do not yet exist but will not have been in electronic storage for 180 days if they are turned over "immediately" The order is statutorily sufficient as to posts stored for more than 180 days, but as held in *Warshak*, that statutory standard is unconstitutional. (That said, *Warshak* is a federal circuit case not directly binding on the Virginia courts, where Aaardvark would need to move to quash.) None of the exceptions in the Stored Communications Act apply; there is no user consent (especially given Aardvark's strong statements about privacy), there is no necessity to protect the rights or property of Aardvark, and the disclosure would be to a governmental entity. Finally, the Stored Communications Act does require Aardvark to turn over the metadata described in § 2703(c)(2);"records of session times and durations" and "subscriber number and identity" probably cover all of the requested categories. Aardvark's only objection here would be that these records are "unusually voluminous." § 2703(d).

Wiretap Act

If Aardvark were to use a modified version of Aarfy to obtain users' passwords, it might be committing a violation of the Wiretap Act. The best counter would be that Aarfy does not

intercept any *communications*, because the passwords are intended to be used only by Aarfy and are never transmitted to Aardvark or other users.

Similarly, if Aardvark were to identify and turn over posts from Yossarian22, that would likely be a violation of the Wiretap Act. The contemporaneity or near-contemporaneity of the acquisition of the contents would make it a Wiretap Act issue. *O'Brien*.

Aardvark's Liability

Aardvark is protected by Section 230 from liability for the actions of its users. Section 230 preempts any state law that would treat Aardvark as the publisher or speaker of content created by its users. The stolen credit-car numbers and posts involving harassment and extortion all fit into this category. Indeed, since AAG Cathcart is an agent of the Commonwealth of Virginia, any liability he could threaten to impose on Aardvark on this basis would be preempted. Section 230 even reaches state criminal laws, so state child pornography charges would be preempted.

Unfortunately, it is possible that AAG Cathcart could make calls to someone who could bring non-preempted claims or charges against Aardvark. Section 230 does not reach federal criminal liability. Fortunately, however, Aardvark's strong encryption provides it a defense to any argument that it possessed child pornography; Aardvark has no idea what content its users are exchanging. Section 230 also does not reach intellectual property, including copyright law. The pirated software movies could potentially give rise to copyright liability for Aardvark. Here, however, Section 512 fills the gap: so long as Aardvark responds to takedown requests (it does not appear to have received any), lacks the right and ability to control users' infringement (which it does because it cannot even distinguish infringing from noninfringing material), and does not have knowledge of infringing activity (which it does not, for similar reasons), it will not be liable for copyright infringement.

Ability to Comply

Aardvark can comply with the portion of the § 2703(d) order pertaining to metadata. This does not require any knowledge of the contents of posts or titles, just the fact that posts have been made and some basic information about their size and by whom. Aardvark has all of this information, including users' IP addresses.

On the other hand, Aardvark, at present, lacks the ability even to identify which forum is Our Name is Mudd and which user is Yossarian22. Even if it could identify them, the relevant posts would be encrypted. Leaving aside the Fourth Amendment and statutory issues, Aardvark could turn over to AAG Cathcart all that it has, and only that: the encrypted versions of the posts. This, it appears, would draw a renewed demand that Aardvark find a way to obtain the unencrypted version, for example using the Aarfy trick. It is far from clear that § 2703 can be stretched that far, although AAG Cathcart may have other weapons up his sleeve. Fighting him now may just mean that he will return with a search warrant or a court order specifically demanding alterations to Aarfy.

Given that Aardvark has taken such a strong pro-privacy position, this is a battle that it must wage; it cannot afford to be seen as having complied with a demand to pierce its users' privacy without having tried its utmost to protect them. It should particularly object to any demand that it subvert Aarfy and trick users into giving up their passwords. Depending on how serious you are about the privacy mission, consider shutting down the service rather than allowing Aarfy to be compromised in this way.

(3) Minder Binder

Identifying a Defendant

As a threshold matter, it is not yet clear who has taken over the minderbinder.com domain and is using it to attack our business. It is possible, and I would guess likely, that this is being carried out by the Daniel Daneeka who works for our competitor Snowden School Supplies. But the evidence is circumstantial; it is also possible that Snowden is being framed by some third party. Bringing a UDRP complaint, as I recommend below, may help flush out the true party in interest. I will also consider simply calling Daneeka directly and asking him about the domain point-blank. I would like to have a stronger basis to be certain that Snowden is involved before filing suit. If necessary, we can subpoena records from the search engines where the ads have been placed, or seek IP addresses from the domain-name registrars. In what follows, I will assume that Snowden is behind the skulduggery taking place.

UDRP

We can and should bring a UDRP complaint seeking transfer of the minderbinder.com and holderfolder.com domain names. Doing so will not prejudice our ability to bring suit, and it could resolve this entire dispute quickly and cheaply. There is no serious question but that each domain is identical to one of our trademarks, and the "legitimate interests" prong collapses into the bad faith inquiry, because the only possible legitimate interest is using the domains for a fansite or commentary on our products (rather than some independent right to use the names). There is a threshold question with minderbinder.com, as it was registered in good faith by Tappman; the switch to an abusive site only came later with the sale to Daneeka. Parsing the UDRP, however, I think we can argue that the "bad faith" element modifies only "is being used" and not "has been registered." We are not bringing an action against Tappman, and we can point

to Daneeka's purchase of the domain name as being equivalent to registering it for all practical purposes. Matters are easier for holderfolder.com, as it was only just now registered.

The crucial question will be showing that each domain "has been registered and is being used in bad faith." UDRP § 4.a(iii). I will draw on United States trademark cases, which although they are not directly binding in UDRP actions, have raised similar issues. This is not a case of pure cybersquatting as in *Toeppen*: the domains are being used for an extensive website (albeit a problematic one). A better argument for us comes from *Doughney*, in which the defendant's website was devoted to criticism and used an identical domain name, thereby diverting users from visiting the plaintiff's website. *Taubman* cuts the other way: there, a fansite was held not to infringe the trademark owner's rights despite using an identical name. But *Sabin* shows that some UDRP arbitrators will treat sites devoted to criticism as bad-faith. The fact that the respondent here also registered holderfolder.com could be used to help establish a pattern of such registrations. In the end, I think we are not likely to succeed, but since the UDRP is low-risk, there is no reason not to bring one.

Trademark Issues

We can sue the new operator of minderbinder.com for trademark infringement of our Minder Binder trademark, based on the numerous uses of the trademark on the site, in the domain name itself, and in the search keyword advertising. One threshold issue that will complicate such a suit is proving that the mark is being used commercially. Snowden's status as a competitor in the school-supplies market is a strong factor working in our favor. We can also point to *PETA v. Doughney* for the proposition that preventing users from reaching our site is a form of commercial use. That theory, however, may not be viable after cases like *Falwell* and *Taubman*. Establishing consumer confusion may be difficult, as no one is buying anything from

minderbinder.com under the mistaken belief that it is our product; indeed, no one is buying anything from minderbinder.com at all. We might be able to argue initial interest confusion, as in *Brookfield*, but again, without purchases through the site, this may be a difficult argument.

In addition, Snowden could claim that the site is a parody or other protected form of commentary. In its original form, the domain was a protected fan site (as in *Taubman*); switching from praise to criticism is not enough to change the fact that the site primarily comments on Minder Binders. The fact that it is being operated by a competitor is a damning fact, however, and a court might be concerned that protecting this site as "commentary" would give competitors free rein to tarnish each others' trademarks.

We might also be able to bring an ACPA action for cybersquatting; this would depend on showing bad faith.[3] And finally, although it is something of a stretch, we might be able to argue that the site runs afoul of § 2252B because it attempts to trick viewers into looking at obscenity. It is not clear that the images on the site, although pornographic, actually constitute obscenity. Indeed, the use of them to comment on Minder Binder may take them out of the category of obscenity by supplying them with redeeming social value.

Copyright

We could attempt to sue for copyright infringement based on the use of our promotional photographs, but that would be subject to a fair use defense on the theory that the images comment (however crudely) on our products. A better tactic might be to reach out to the record labels and invite them to take action over the unauthorized posting of their music videos. At the very least, they could send § 512(c) notices to have the videos taken down; if the site has no DMCA agent or failed to respond, they might be able to show that it should be held secondarily

[3] Because we did not dwell on the ACPA, I did not expect extensive discussion of it. I gave full credit for discussing the bad-faith factors regardless of whether you

liable for the infringement. Given the active management of the site to promote derogatory content, it might well be inducing infringement by the users who upload the videos—the relevant facts could come out in discovery.

Miscellaneous Torts

The users who posted about their negative experiences with Minder Binder products may be committing trade libel by making false claims about the harms our products have caused. The post about a Minder Binder attacking the user's grandmother may be obvious hyperbole, but the claim that a broken ring could cut a user's finger could be both false and damaging. Unfortunately, Section 230 shields the operators of minderbinder.com from tort liability for user-created posts like these. Even the fact that minderbinder.com seems to be selecting which posts to allow to remain in bad faith will not undermine its immunity: Section 230 protects decisions to filter as well as decisions not to filter. That said, should it come out in discovery into the trademark claims that some of these materials were posted by Daneeka or another Snowden employee, then they would not be "information provided by *another* information content provider." We should add the posters as John Does to the suit, if we file one, so that we can potentially add them later as parties by taking discovery into their identities.