Internet Law
Spring 2022
Final Exam

I graded your essays as follows:

- Correct and complete legal analysis: 70%
- Strategic advice: 15%
- Clarity and organization: 15%

The bullet points in the following outline do not directly correspond to my grading rubric, but they do reflect the overall weight I put on different parts of the analysis. I awarded full credit for identifying an issue and analyzing it carefully even if you reached a different conclusion than I did. Indeed, in several cases I awarded bonus points for spotting an issue I missed, or for surprising me with an argument I had not thought of.

I will of course be happy to discuss your essays and your grades with you if you have any questions.

Question 1: The Time-Wasting Machine

Most of Morlock's ideas are terrible, but Vermont's and Brazil's are even worse.

Subpoenas

Morlock's plan to disclose user information in response to civil subpoenas violates the Stored Communications Act.

- Blurter *can* disclose customer records to in response to subpoenas. 18 U.S.C. § 2702(c)(6).
- Blurter *can* disclose blurts from accounts whose users make their blurts public, as the users have consented to this disclosure. *Ehling v. Monmouth-Ocean*.
- Blurter *cannot* disclose users' direct messages, as these are "electronic communications" that are "in electronic storage," 17 U.S.C. § 2703(a)(1), and no SCA exception applies. Blurter does not have user consent, and it is it is not protecting its rights or property.
- Blurter is not obligated to give affected users the opportunity to move to quash the subpoenas, but failing to do so may be bad for customer relations.

Morlock's plan to disclose user information in response to informal requests from law enforcement also violates the Stored Communications Act.

- Blurter *cannot* disclose customer records to a "governmental entity" without at least a (d) order. 17 U.S.C. § 2703(c).
- Blurter *can* disclose blurts from accounts whose users make their blurts public, for the same reasons as above.
- Blurter *cannot* disclose users' direct messages, for the same reasons as above.
- Any information disclosed this way will likely be excluded as having been obtained in violation of the Fourth Amendment. *Warshak*.

Copyright

Morlock's proposed 48-hour hold exposes Blurter to potentially massive copyright liability.

- Blurter has a safe harbor under § 512(c) of the Copyright Act for user-posted content, as long it "responds expeditiously to remove, or disable access to" that content when it receives an infringement notice.
- While a 48-hour response time might be considered "expeditious[]" under some circumstances, a court could find that a deliberate 48-hour hold is by itself an unreasonable delay. In addition, it is possible that some types of infringements (e.g. for ongoing live events) might be held to require more prompt action.
- The danger for Blurter is that many of these infringement notices will concern activity that is blatantly infringing, and for which Blurter will have no good defense on the merits.

Morlock's proposal to sue ten copyright owners is not likely to yield concrete results.

- Morlock is correct that many takedown notices are filed against material that is obviously non-infringing, or for which the sender does not hold the copyright.
- Section 512(f) of the Copyright Act authorizes suits by parties who have been harmed by knowing material misrepresentations in a takedown notice.
- Unfortunately, under *Lenz*, even an unreasonable belief by a notice sender will immunize them from liability under § 512(f).
- Suing a few particularly abusive senders will not result in substantial damages, nor will it deter high-volume senders whose individual claims are not egregious.

Morlock's proposal to reincorporate in the Seychelles will not shield Blurter from copyright liability.

- The Copyright Act gives United States courts subject-matter jurisdiction over cases of infringement where the recipient is located in the United States, regardless of where the sender's servers or headquarters are. *Spanski Enterprises*.

- Blurter has employees, operations, and many millions of users in the United States, so it is subject to personal jurisdiction here.
- Blurter has assets in the U.S.ANo that can be seized.

Ad Blockers

Morlock's proposal to sue SuperBlocker will not work.

- I will assume that Blurter's signup process is sufficient to bind users to its terms of service, as amended to include the anti-adblocking clause. If not, it can be revised to force all users to specifically agree to the amended terms to continue using the service.
- Unfortunately, SuperBlocker does not itself access Blurter and has never agreed to the terms. Unlike LineJump (see the LineJump Problem), which directly accesses the company's servers, SuperBlocker runs in a user's browser (see the Cookie Monster problem).
- Following *Van Buren* and *HiQ*, it is unlikely that either the users or SuperBlocker are violating the Computer Fraud and Abuse Act. Users' browsers access portions of the website to which Blurter has specifically allowed them access; indeed, most of those portions are entirely public.

Eddie Prendick

Morlock can delete Prendick's account with impunity.

- Section 230(c)(2) gives interactive computer services, such as Blurter, immunity from any claim for actions taken to restrict access to material the provider considers "objectionable."
- Some courts read this provision broadly, covering any removal for any reason. Others, such as *Song Fi I*, say that removals can only be for "obscene, lewd, lascivious, filthy, excessively violent, [or] harassing" content.
- But even if Section 230 does not immunize Blurter, it is unclear what causes of action Prendick could bring. *Song Fi II*. Blurter's terms of service either preclude or can be amended to preclude any user suit for removing content.

- In addition, Blurter has a strong First Amendment argument that it is entitled to choose what speech it will carry on its platform. *Zhang v. Baidu*.

Vermont

Blurter can probably ignore the Vermont law.

- Section 230(c)(1) protects Blurter from liability for any user-provided content it carries (i.e. hollow-earth content that Blurter leaves up). None of the exceptions in subsection (e) applies to the Vermont law; indeed subsection (e)(3) specifically preempts inconsistent state law.
- Section 230(c)(2) protects Blurter from liability for any user-provided content it removes (i.e. anti-hollow-earth content that Blurter takes down). As above, Blurter can argue that such content is "otherwise objectionable."
- As above, Blurter can argue that it has a First Amendment right to exercise editorial discretion over the speech it carries.
- In addition, by requiring the removal of hollow-earth content, the Vermont law violates the First Amendment rights of Blurter users — both as speakers and as listeners.
- Blurter might choose to take down such content, but it should decide whether do so in light of its users' needs and its desire to contribute positively to society.
- If Blurter does decide to act, it will be difficult to decide which content is hollow-earth denialism, and it will probably require substantial human moderation effort.

Tractors

Blurter can probably ignore the Brazilian tractor issue, but it may or may not be a good business decision.

- Morlock is correct that Brazil is unlikely to be able to obtain an enforceable judgment. Under the First Amendment and Section 230, U.S. courts will probably deny recognition to any such judgment entered in Brazil. *Equustek II*.
- Brazil, however, might retaliate by attempting to block Blurter in Brazil. If this is a market that is important to Blurter, its lack of physi-

cal presence notwithstanding, this may be a fight Blurter is unwilling to provoke.

- If Blurter does attempt to block tractor photos, it will need to use a combination of content filtering (to detect images with tractors) and geofiltering (to allow such photos elsewhere but not in Brazil). Both types of filtering are leaky, so there is a risk that some images might make it through nonetheless.

Question 2: My Private Key is My Passport

This is the worst security crisis in the history of the Internet.

Stripe

- Users' communications with Stripe's servers are "electronic communications." 18 U.S.C. § 2510(12).
- SETEC "intercepts" those communications when it observes their contents (credit card numbers, payment amounts, etc.). *Id.* § 2510(4).
- SETEC's interception is "by means of a device," i.e. the computers with which it connects to public WiFi networks. *Id.* § 2510(5).
- These communications are not "readily accessible to the general public" because they are HTTPS-encrypted. *Id.* § 2511(2)(g)(i).
- Thus, SETEC violates the Wiretap Act when it intentionally intercepts these communications. *Id.* § 2511(1)(a).
- In addition, if SETEC makes unauthorized use of these credit card numbers, its members are likely committing theft and/or fraud.
- There is no Computer Fraud and Abuse Act violation, because SETEC did not "access" either users' or Stripe's computers. While it did access the public WiFi routers in connecting to and exchanging messages with them, this access was authorized by the providers of public WiFi, who enabled any member of the public to make this kind of access. *See HiQ*.

State Department

- Most of the analysis of State Department officials' diplomatic messages are the same as above.
- SETEC could argue that the officials intentionally shared their messages with SETEC's server. Thus, SETEC is "one of the parties to the communication," so that its activities fall under the party-consent exception to the Wiretap Act. 18 U.S.C. § 2511(2)(d).
- On balance, however, SETEC's deliberate impersonation of the State Department server, by means of the State Department's private key, suggests that SETEC should not be regarded as one of the parties.

The officials were tricked into thinking they were communicating with someone else. (*Cf.* Question 1 on page 260 following *O'Brien*.)

Robert Bishop

- Bishop's Bitcoin are property under the *Kremen* test. They are capable of precise definition (the blockchain keeps track of who owns which Bitcoin), they are capable of exclusive possession and control (via private keys), and Bishop had a legitimate claim to exclusivity (via his private key).
- Thus, when SETEC transferred Bishop's Bitcoin to its own address, it committed the tort of conversion and the crime of theft.
- This was probably not a CFAA violation, because the only computers SETEC affected were the miners' computers collectively making up the blockchain. Those computers agree to record any transaction signed with a valid private key, so any access to them is with authorization.

Google Play

- The Google Play DRM "effectively controls access" to copyrighted works (books, movies, music, etc.) because it requires the use of decryption keys to gain access to those works. 17 U.S.C. § 1201(a)(3)(B).
- When SETEC decrypted those works with the private keys it generated, it violated the DMCA. *Id.* § 1201(a)(1)(A).
- Cosmo may have violated the anti-trafficking provisions of the DMCA, because the private key they provided to SETEC was both "primarily designed or produced" to circumvent the Google Play DRM, *id.* § 1201(a)(2)(A), and "has only limited commercially significant purpose or use" other than circumventing Google Play DRM, *id.* § 1201(a)(2)(B). Cosmo has a plausible defense to the first theory in that *they* did not design it for circumvention because they did not know what it was for or how it would be used.
- When SETEC sold the decrypted media, it violated the Copyright Act's prohibitions on reproduction and distribution of copyrighted works without the permission of the copyright owner.

Lee Rhyzkov

- SETEC violated the CFAA by installing its software on Rhyzkov's iPhone. The iPhone is a protected computer, SETEC accessed it by installing the update, and the access was "without authorization" because the use of the private key bypassed the security measure intended to prevent installation of non-Apple updates.
- Specifically, SETEC violated section (a)(2)(C) of the CFAA by obtaining information from Rhyzkov's iPhone. If its insider-trading is regarded as a "scheme to defraud," it also violated section (a)(4) of the CFAA.
- SETEC's insider trading likely violates federal securities laws.
- By observing Rhyzkov's professional communications (likely including attorney-client protected matters), SETEC committed the tort of intrusion on seclusion.

Crimes and Civil Suits

- SETEC has violated the Wiretap Act (as to Stripe and its users, and as to State Department officials), theft laws possibly including the federal wire fraud statute (as to Bishop), the Copyright Act and DMCA (as to Google Play), the CFAA (as to Rhyzkov), and the securities laws.
- Whether Cosmo violated these laws depends on their knowledge about how SETEC would use the keys. Cosmo's outreach to an underground group, the arms-length nature of the transaction, and the high price per key all suggest that Cosmo was being willfully blind to the specifics of SETEC's unlawful activity, and should therefore be treated as having knowledge of them.
- Cosmo may also have committed money laundering, although taking payment in Bitcoin is not by itself money laundering.
- Bishop can sue SETEC for conversion, Google can sue for a civil DMCA violation, the copyright owners can sue for copyright infringement, and Rhyzkov can sue for intrusion on seclusion.

Identifying Cosmo

- The FBI has probable cause to obtain a search warrant for the werner_brandes@gmail.com account. As described above, there is ample evidence that crimes have been committed, and the identity of Cosmo is central to prosecuting them.
- The FBI should obtain a search warrant and serve it on Google to obtain the complete contents of the account, as well as any customer records (such as IP addresses, contact information, or credit-card information) about Cosmo.
- The FBI should also obtain a search warrant for the list of users (or IP addresses) that have downloaded the Astronomy library from GitHub. Since the list is so short, it is worth looking for any connections to the information Google has.
- The FBI can also watch the Bitcoin addresses used by Cosmo and SETEC for transactions. If they attempt to exchange those Bitcoins for real-world money, these will provide additional leads.

Janek

- Like Snuffle in *Bernstein*, the Astronomy library is software with a speech component (informing others about mathematics), so it is covered by the First Amendment.
- It does not appear that the Astronomy library by itself can be used to obtain private keys; some further technique (which Janek may not know) is required.
- Given these facts, the FBI will probably not be able to get a court to order Janek to remove the Astronomy library from Github.
- However, because the library is obscure and has not been downloaded often, it might be possible to persuade Janek to voluntarily take the library down while the investigation continues.
- At any rate, this is not the FBI's top priority, at least as long as Cosmo and SETEC are active, because if Cosmo's secret spreads, the damage will be much more far-reaching.

General Advice

- The FBI has an urgent and massive security crisis on its hands, because of the risk that Cosmo's private-key-extracting method could become widely known. If so, then Internet security *for everyone in the world* would be immediately undermined in all of the ways SETEC has compromised it for a few. This would be a catastrophe, and the FBI's top priority must be to prevent it from happening.
- If Cosmo can break public-key encryption like this, someone else will be able to, and others may rediscover the same attack quickly once they realize someone has done so. The FBI is extremely unlikely to be able to keep this knowledge bottled up forever, only to delay its general public release for a bit.
- The FBI needs to urgently convene security officers from companies and open-source groups providing this cryptographic infrastructure and work with them to develop and deploy replacements on an all-hands-on-deck basis.
- The FBI may need to trade off the operational goals of prosecuting Cosmo and SETEC against these broader security concerns. Arresting them may signal what is happening to others. But the longer the FBI waits, the greater the chance they will leak the information on their own. On the other hand, if the FBI acts to close these new vulnerabilities, Cosmo and SETEC may realize that their secret has been discovered and seek to cover their tracks.