UNIVERSITY OF NEW HAMPSHIRE SCHOOL OF LAW
PROFESSOR TIFFANY LI

INTERNET LAW
FALL 2021 – FINAL EXAM SAMPLE ANSWERS

The following are real student responses, taken from different student exams. While these were generally high-scoring answers, none are necessarily perfect answers. (Rest assured that there are few, if any, perfect answers on any exam ever.) Some sample answers include irrelevant information, grammar or spelling mistakes, odd formatting, etc. Some even include mistakes in legal analysis. Please do not use these as factual study guides but as examples for reference.

Table of Contents

Question 1: Petrichor Vote

Sample Answer A

While likely legally allowable, if Petrichor wishes to be seen as an ethical and responsible company, it should deny the request from the campaigns.

Petrichor is a private company and thus its speech is protected under the first amendment. Further, Section 230 of the Communications Decency Act protects interactive computer services, like Petrichor, from being deemed liable for the speech on its service, including any moderation it chooses to partake in. Thus, under Section 230, Petrichor is legally able to moderate the chat as it sees fit. However, it should be noted that the actual moderation would be "at the will and discretion of the candidates." Glinda Goverson, one of the candidates, is a sitting public official and that raises some concerns.

Generally. government officials cannot abridge the rights of individuals in the United States, and there could be an argument that should she employ the technology of blocking a constituent during the debate, doing so is a violation of that constituent's First Amendment rights. This argument likely fails for two reasons. 1) Glinda would not be acting in her official capacity as governor; and 2) it is not her personal page that is being used as an organ of official business.

First, Glinda is not acting in her official capacity as governor, instead acting as a candidate for a position in office as a private citizen. The Constitution only applies to government actors, and as such Glinda acting as a private citizen would not be able to be held liable for blocking constituents during the debate.

Further, even if Glinda should be deemed to be acting in her official capacity as governor, a court could find that this would not be her personal account and would not be held liable. Courts have found that even in cases where the defendant-official is acting in their official role, if they are using accounts that are not an "organ of official business" the official has the prerogative to select their audience as they see fit. (*Campbell v. Reisch*). While other courts in different circuits have found anytime an official is acting in their official capacity and create an "open forum," they are unable to block certain users, these types of cases are easily distinguishable. (*See Knights First Amendment Inst. v. Trump, GIL 126*) In cases like *Trump* the accounts are used for notification of official policies and as an "official vehicle of governance." The same cannot be said in our case. Glinda is not using the debate to announce policy, hear constituent feedback, or discuss the goals of the current government. Instead, she is making her pitch to get reelected, detached from the current office she holds. Thus, it is unlikely that a court would find her liable for blocking the constituent.

In any event, it is unlikely that *Petrichor* will be held liable for the blocking of users in this instance. However, despite the low likelihood of liability, it is a cornerstone of American democracy that the right of free speech be upheld. Thus, it would be important to note that instituting the ability to block individuals would be a bad look for the company – especially when looking to be viewed as an ethical and responsible company. Thus, while legally allowable, I would advise that Petrichor only block users from the live stream and comment section that are engaging in hateful comments or spamming the system, and only allow Petrichor moderators to do so.

Sample Answer B

Petrichor likely will not likely face legal liability for installing a blocking function that allows political candidates to restrict users from accessing the livestream and comments section. However, Petrichor will likely face public retribution and negative market consequences if it is branded as a platform that unnecessarily censors political speech or viewpoints.

Section 230 grants immunity to interactive computer services, where they are not liable for information that originates from third parties. *Zeran v. AOL*. Section 230 also creates a safe harbor, which permits content providers and others to restrict third-party content and users on the platform in question. 47 U.S.C. 230(c)(2)(B). Courts apply a three-part test to determine if Section 230 bars liability. Courts ask: 1) is the defendant a provider or user of an interactive computer service? 2) Does the plaintiff seek to hold the defendant liable as a publisher or speaker? 3) Does the plaintiff's claim arise from information provided by another information content provider? If the answer to any of these questions is 'no,' then Section 230 will not bar liability. Content providers and others may restrict content "in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd… or otherwise objectionable." 47 U.S.C. 230(c)(2)(A).

Like the case in *Zeran*, where AOL, an internet service company, was not liable for curating third-party content found in its platform, Petrichor, which also provides an interactive computer service, would not be liable for curating third-party content found on the platform. Petrichor would very likely pass the three-part test. Under 230, liability does not change whether Petrichor, or the political candidates are the ones editing or restricting content and users on the platform. Affected parties may sue Petrichor or the politicians if they believe they were restricted from the platform in bad faith, but such accusations require discovery, are expensive and time consuming, and typically are unlikely to occur. Even with potential, politically motivated and funded plaintiffs, neither Petrichor nor the political candidates are likely to be found in violation of Section 230 because the bar is a high one. However, the inevitable negative publicity, and the time and effort required to deal with such suits may not be worth the trouble. As the saying goes, "the process is the punishment."

Section 230's protection is not limitless. It applies only to the extent that an interactive computer service provider is not also the information content provider of the content at issue. *Jones v. Dirty World Entertainment*. To make this determination, courts apply the material contribution test, which asks if an editor materially contributed to third party content or unprotected activity. Similar to *Jones*, where the court found that the website editor did not materially alter third party posts and thus was protected under Section 230, Petrichor would be protected under Section 230 because a blocking function would not materially edit posts or other content. There are also exceptions to Section 230, such as content that falls under federal criminal law, federal intellectual property law, and ECPA, but these exceptions are not likely to be found in a political debate forum. Similarly, some states have passed legislation, e.g., Florida's SB 7072 and Texas HB 20, which may potentially conflict with Section 230 and/or Petrichor's

political debate platform. Although Section 230 likely preempts state laws that deal with content moderation, there may be future legal battles in some states regarding Petrichor's blocking functions.

More to the heart of the matter, although neither Petrichor nor political candidates are government entities, and so they are free to restrict or enable speech how they see fit on the platform, Petrichor should be wary of First Amendment concerns regarding its debate forum for political candidates. Similar to *Packingham v. North Carolina*, where the court found that internet platforms such as Facebook, etc. were 'quintessential public forums,' Petrichor's pre- election debate forum may potentially be viewed by the public, legislative bodies, and even courts as a public forum (subject to the First Amendment) rather than a private one (not subject to the First Amendment). This is particularly likely if Petrichor's platform becomes successful such that alternative options to view or host such political debates are diminished. If Petrichor's pre-election platform should be legally considered or made a public forum, then censored individuals may sue Petrichor or the politician-in-question for violating their First Amendment rights. They would not likely win if they are found engaging in viewpoint or content-based discrimination, especially in the context of electoral politics. For similar reasons, Petrichor should be wary about dealing with private actors working on behalf of the government. Incumbent political candidates should be notified not to conduct official government business through Petrichor's political platform lest they be liable to lawsuits under the First Amendment or other laws. *See Campbell v. Reisch*.

On a final note, because free speech in politics is a deeply ingrained American norm, if Petrichor is seen as a platform that allows unnecessary censorship, it will likely create a public backlash against the platform for skewing or restricting access to information pertaining to elections. This will have noticeable market and reputational effects for Petrichor regardless whether legal liability applies.

Question 2: MrBonez411

Sample Answer A

Petrichor's United States legal risks for MrBonez411's actions are minimal, and they are largely protected under Section 230. Section 230 protects providers of an "interactive computer service" from being treated as the publisher or speaker of information that was asserted by another information content provider, or user. (*See* Section 230(c)(1)). Section 230 defines "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server…" Petrichor would qualify as an interactive computer service capable of Section 230 protection where they provide a platform for third-party users to live-stream both video and audio, and provide for direct and group messaging. The activities of MrBonez411 are his own, and Section 230 protects Petrichor from liability that would result if they were responsible for the messages of an unrelated entity.

Section 230 immunity is not endless, and there are certainly additional foreign law considerations.

U.S. Legal Risks & California Law

While there is not a federal prohibition, the state of California has banned the sale of human remains. This presents an additional element for consideration because the actions of MrBonez411 are considered illegal in this state, a state where Petrichor has a large presence and many users. In *Zeran v. America Online*, an anonymous user utilized AOLs interactive computer service to pose as Zeran, encouraging people to call him with complaints as he was advertising merchandise with offensive phrases relating to a recent local bombing. *Zeran* attempted to argue that AOL should be liable as a distributor of this content, because distributors are liable for knowingly distributing illegal material. However, the court ruled in favor of AOL where Section 230 prohibits holding AOL liable as publishers or distributors, therefore despite the illegality of the actions taken by the 3rd party, AOL is protected. This ruling favors Petrichor, as it suggests that despite the illegality of MrBonez411's actions within the boundaries of state of California, Petrichor as the interactive computer service should avoid liabilities for the actions of the 3rd party.

The outcome varies in the *Roommates* case, which also addresses concerns of illegal content on the internet. In contrast to *Zeran*, the defendant, Roommates.com, was ultimately held liable for knowingly inducing the illegal content from the 3rd party users, where the website *required* users to provide information in violation of the Fair Housing Act and the California Fair Employment and Housing Act (the information including sex, sexual orientation, and familial status.) The court held that despite their status as a interactive computer service, Roommates.com was not entitled to immunity where they actively required users to submit the illegal information.

The critical difference between *Zeran* and *Roommates* was whether or not the website owners induced or materially contributed to the illegal activity. Therefore, unless there is evidence that Petrichor actively induced MrBonez411, they should not face a legal risk in the United States for his action

Foreign Legal Risks & French Law

Unfortunately, Section 230 does not extend outside the United States borders and French law renders the sale of human remains a crime. Perpetrators of this crime include both parties who directly and indirectly facilitate or support the sale of human remains and may result in a large fine or potential jail time. We have French precedent dictating potential French reactions if Petrichor were to ignore MrBonez411 behavior, allowing the continuation of the sale of human remains. In the early 2000s, French antiracism groups sued Yahoo for violating the French law against the sale and trafficking in Nazi goods, where Yahoo was hosting websites which facilitated the sale of such goods. Yahoo attempted to ignore this, but were summoned to French trial court, which ultimately ruled that Yahoo was in violation of the existing law and ordered Yahoo to take down these websites. Yahoo attempted to argue ignorance and inability to

discern between users locations; when this proved untrue, illustrated by Yahoo was able to dictate specified advertisement an language settings between countries, France ordered Yahoo to

comply. The court acknowledged that 100% blocking was impossible, and ruled that they must assert their best effort. It should be noted that Yahoo wanted to ignore this, but they had assets in France and income from a French subsidiary, so ultimately they complied.

In deference to this precedent, it is in Petrichor's best interest to do *something* regarding MrBonez411's actions if they wish to continue to promote and grow within France. Clearly, their presence in advertising and desire to grow establishes some presence in France, likely giving France *some* authority and jurisdiction. However, there may be some loopholes regarding jurisdiction where unlike Yahoo, it doesn't seem Petrichor has a large presence. There seems to be some direct interaction, depending on the French rules of jurisdiction Petrichor may be liable. To avoid this, I would recommend utilizing the standard of best effort, to reduce or eliminate the conduct of MrBonez411, at the very least in France. The French case involving Yahoo discussed the potential for Yahoo to reroute specific websites with legal violations in France, solely avoiding French citizens. Given the nature of Petrichor's business model, being a video sharing/chat room host (as opposed to Yahoo which hosted entire websites), it may be more difficult to preclude this behavior only from France.

If Petrichor wishes to remain neutral and continue to let MrBonez411 continue, they should attempt an architectural remedy to remove his account/actions from French users. If this is impossible, they may want to remove MrBones411 and explicitly prohibit this behavior in an updated TOS. The legal ramifications for the existing behavior for Petrichor are minimal in the United States, but may result in legal issues in France or other foreign nations. Because of this, the final call is one of business and strategy. I would suggest prohibiting this type of conduct, as it likely does little to benefit the website as a whole and has a large potential to end in legal ramifications, or public good will ramifications; Petrichor also specifically asserted that to prove itself to potential investors, they would like a positive public image as an ethical and responsible company. Because of this, I would recommend removing MrBonez411, which they are legally allowed to do as a private company, and can site their TOS as reason enough, which prohibits illegal activity on the website.

Sample Answer B

Risk of criminal liability

Because MrBonez411 is doing his business selling of human bones on Petrichor Chat, there is a risk that Petrichor is criminally liable for aiding or abetting a crime, at least in California and France, where selling human remains is criminalized.

In this context, the first question would be whether there is a criminal jurisdiction over Petrichor.

In California

As for California, the court assesses whether it is a proper venue considering circumstances such as the residents' domiciles and where the criminal conduct occurs. (*United States v. Auernheimer*, a NJ court rejecting the venue because defendants are not NJ residents, server is not in NJ, conduct occurred not in NJ; *In re Facebook Biometric Information Privacy Litigation*, a IL court holding the state statute constitutional and finding criminal jurisdiction over Facebook).

However, assuming, arguendo, a criminal jurisdiction is found over Petrichor in California, Petrichor would be able to argue for intermediary immunity under Sec 230 for internet service providers like Petrichor from liabilities related to speeches or conducts made by users of the service.

Sec 230's applicability has exceptions which include that it does not apply to federal crimes and infringement of intellectual property cases. However, for selling human remains, there is no federal criminal law, but only California state law. Therefore, Sec 230's immunity will apply to Petrichor in this case and Petrichor will be able to establish its defense in a potential criminal case against it in California court for aiding and abetting selling human remains.

In France

However, as for France, the statute clearly stipulates that "any party that directly or indirectly facilitates or supports the sale of human remains can be punished."

Also, because Petrichor is advertising heavily in France and actively trying to grow the business in France, it may be said that Petrichor is purposefully avail itself under the jurisdiction of France. Therefore, if Petrichor is accused in a French court, the court would likely conclude there is a criminal jurisdiction over Petrichor.

Thus, assuming there is no immunity law in France corresponding to Sec 230, there is a risk that Petrichor is punished under the aforementioned French law.

Therefore, Petrichor is advised to take action to remove such activities of selling human remains from its platform.

Good Faith Activities for Removing Contents Under Section 230(c)

In doing so (i.e., removing such activities and related contents) without consent of or notice to MrBones411's, Petrichor may use Section 230(c) as its legal ground, which provides civil immunity for such action of removal (i.e., no civil liability for 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.)

Petrichor may argue that the conduct of selling human remands and related contents are included in "otherwise objectionable", and therefore its activities to remove those are in good faith, protected under Sec 230(c).

Breach of Contract claim against MrBonez411

Furthermore, Petrichor may make a breach of contract claim against MrBonez411 because Petrichor's Terms of Services stipulates a user "agree not to do anything illegal or harmful using our website or applications" and Petrichor breached the ToS by violating California statute prohibiting selling of human remains.

As a point to take a note, MrBonez411 may try to make an argument that Petrichor's Terms of Service is not valid. The courts in the U.S. hold the validity of online service's Terms of Service if it is reasonably conspicuous. The courts consider the manner inviting users to agree to the ToS (e.g., "click-wrap", "browse wrap"), webpage arrangement, visibility of the ToS, contemporaneousness of the agreement, etc. (See. *Meyer v. Uber (2nd Cir, 2017)*, finding the validity of Uber's ToS; *Cullinane v. Uber (1st Cir, 2018)*, denying the validity of Uber's ToS).

In our case, we do not have sufficient information on a manner of inviting agreement, a design, an arrangement of Petrichor's ToS. Thus, as for the question of the validity of the ToS, we would need more facts.

Conclusion

In considering the risk of criminal liability, Petrichor is advised to remove the conducts of selling human remains and related contents from its platform and to consider a breach of contract claim against MrBonez411.

Question 3: PetrichorHatesWomen.com

Sample Answer A

a. Legal position on PWH.com:
The website PetrichorHatesWomen.com (PHW.com) is called as a "**gripe site**" and would fall under fair use one's trademark. Therefore PetrichorHatesWomen.com did not illegally use their intellectual property ie. their trademark.

In the case **Taubman v Webfeats,** the court said that, in internet parlance a web name with a "sucks.com" moniker attached to it is called as "cybergriping". In the Taubman case the plaintiff held that the intention of the defendant was to harm them economically and that all cybergriping sites are per se "commercial" as they are "in connection with the sale of goods". The court rejected this argument and held that though economic damage might be intended, the First Amendment protects critical commentary when there is no confusion as to source, even when it involves the criticism of a business. Such use is not subject to scrutiny under the Lanham Act. The Court held

that domain names public expressions similar to billboard or pulpit and therefore they are protected by First Amendment rights.

Therefore, it there is no actionable claim against PetrichorHatesWomen.Com as it is **not a commercial site,** and there is clear addendum to show that the domain name does not belong to Petrichor. Moreover, the site itself has a disclaimer which says that the website is not affiliated with Petrichor. Such criticism or opinion based sites are protected by the First Amendment.

b. With regard to the username and profile photos which was scrapped from Petrichor's Chat website, an argument can be made that PHW.com violated the Computer Fraud and Abuse Act by violating Petrichor's TOS which explicitly bars scrapping information from its website and thereby has accessed their data "Without authorisation".

It is highly unlikely that Petrichor would succeed in an action against PHW.com under the CFAA. In the case of **HiQ v LinkedIn** the court held that Section 1030 of the CFAA only prohibits the unlawful access of **private information.** Information for which access is granted and is open to general public, permission is not required. In the present case Username and profile photos were publicly available to any visitor to access the Petrichor Chat website. There was no password or security that was circumvented by PHW.com. Therefore there is no actionable claim under the CFAA.

However, Petrichor is not without any remedy. Their very brief TOS mentions that one agrees to not access the platform through automated means include scraping. Therefore, there could be a claim against PHW.com for violation of contract.

c. With regard to the allegations of Petrichor creating a harmful environment for women:

Petrichor would be immune to such allegations as per the Section 230 of CDA. Petrichor is not a "Developer" in the sense that they do not assist in any way for the harassment or the cyberbullying to occur. In the case of **Doe v Myspace,** the main argument of the Plaintiffs against Myspace was that they had failed to undertake safety measures to protect minors on their platform. They claimed that this did not have anything to do with Myspace being a publisher and therefore Section 230 does not apply. However, the court rejected this argument because Myspace published the information of the parties which led to the assault and therefore the claim was eventually directed at Myspace's publisher role. In this case similarly Petrichor would be protected under Section 230 of CDA.

The Petrichor site is not developed in a way to enable harm to the women online. The Victims are unlikely to succeed in an action against Petrichor. However, since the reputation of the website is on the line it is advised that Petrichor make changes to their websites to offer more protection for the vulnerable users on its websites and take active part in investigating into cyberbullying incidents.

Sample Answer B

It is assumed that Petrichor has an active trademark for both Petrichor and Petrichor Chat.

There are three main issues that are presented with this issue. 1) The web-scraping of Petrichor Chat users' information; 2) The website PetrichorHatesWomen.com; and 3) The alleged sexist and harmful environment on Petrichor Chat. I will address each below.

First, while there are minimal legal risks in regard to the website PetrichorHatesWomen.com being up and operated, there are substantial good-will risks associated with such a site being published on the internet, for obvious reasons. However, it is likely that the website is perfectly legal. The only reasonable avenue to take down this website would be to argue that it is a violation of the Lanham Act, an infringement upon Petrichor's trademarks. However, this argument likely fails because under the Lanham Act, a use of another's trademark must be likely to cause confusion, mistake, or deceit. In this instance there doesn't seem to be any support that this would create a likelihood of confusion regarding the ownership of the site. There is a clear disclaimer on the site that explains that there is no affiliation with Petrichor, and courts have found similar uses of trademarked names with additional monikers such as "sucks" creates the understanding that the trademark owner is not the proprietor of the website. *(See Taubman*). While the website is soliciting donations and contains other economic activities, without the likelihood of confusion, there is no claim under the Lanham Act. Thus, the website can likely stay up legally.

Secondly, the web-scraping issue raises some concerns in regard to user data, but likely does not have a legal remedy. The only viable avenue to stop web-scraping is to bring a claim under the Computer Fraud and Abuse Act (CFAA) alleging that the individuals responsible did not have authorization to obtain such information via web scraping. Fortunately, there is precedent that discusses this exact legal issue. Under *Van Buren v. United States* the law is clear in this regard. Exceeding authorized use is not a violation under the CFAA, unless there is some technical barrier in place to prevent access. Petrichor Chat's users' usernames and profile pictures are available to any visitor who accesses the website, regardless of whether the visitor is registered or signed in. Thus, there is no technical measures in place to stop the web-scraping besides a clause in the Terms of Service, an effort the court deemed insufficient in cases like *HiQ Labs v. LinkedIn*.

While the court in *HiQ Labs v. LinkedIn* found that even after instituting technical barriers was insufficient for public information, the case is being reheard after the *Van Buren* case was issued – leading to some confusion about this issue. In the meantime, to protect the information from being web-scraped, it is recommended that technical barriers be put in place that block web- scraping activities, and we can issue a cease-and-desist letter to those responsible. Unfortunately, this is the best advice I can give until more guidance is given by the court.

Lastly, in terms of the sexist and harmful environment alleged by the group, it once again is unlikely to cause legal risk. In general, under Section 230 of the Communications Decency Act, interactive service providers are deemed not to be the publisher of content created by third

parties. While there are some exceptions, it does not seem that any of those apply to the current situation. Further, even in cases where the website has been much more active in choosing which content to post, courts have found Section 230 protections. For a service to not be afford Section 230 protection, the service needs to be "in part responsible for the creation or development of content." In this case, there is no evidence that Petrichor is in anyway contributing to the content other than letting users post or message it. With this, there is minimal legal risk regarding the current situation.[1]

However, it is understandable that Petrichor would want to implement changes to address the allegations. The good news is, Section 230 protects Petrichor from being held liable for that, too. Under Section 230, even if a provider chooses to moderate some aspects of the content, they are not deemed to be the publisher, which means that Petrichor is able to make modifications to its moderation policy to address these concerns. This is a business decision, and with that I would defer to leadership to see what changes they think should be made, but they have latitude in the moderation of the content.

Question 4: Petrichor Face

Sample Answer A

Question 4

Petrichor Face is a bad idea. Petrichor should not proceed with this plan, for three main reasons. Additionally, separate from the legal issues, Petrichor should be aware that machine learning can result in systemic bias based upon the training data set, and should be mindful of the impact their actions can have in creating the software if not done properly.

I. Violation of Open-Source License
Petrichor has used an open-source software in order to develop their facial recognition

software. This is likely a copyleft license because it provides additional rules to a permissive license. Just like a normal licensing agreement, if Petrichor uses the licensed product they must follow the requirements. The conditions of using the software prove that the same permissions are provided to all copies or substantially similar portions of the software, and that the software is not used in whole or in part for any illegal, unethical, or immoral purpose.

Petrichor Face is likely an immoral use of the software. It is being created secretly by using data that Petrichor is taking from their customers without there consent. Although Petrichor has a right to the content as stipulated in their terms of service, they give no notice of this purpose, and their terms of service is questionable as discussed above.

Additionally, they would not be providing the same permissions when they sell their software. They plan to secretly sell this to military and law enforcement buyers around the world. They clearly do not intent for this software to be open like the software they are basing it upon.

Because they are not following the terms of the copyright license, they may face legal issues if FreeFlow choses to enforce it. Additionally, a lack of respect for the license could ostracize future potential workers who are in favor of the open-source movement.

II. Employee Whistleblowing
Petrichor should also be concerned with not offending current employees. They may choose to inform the press or the government of the plans, despite the NDA. Even though the NDA is likely grounds to sue any whistleblowing employees, that would be very bad for the organizations reputation, and make people less willing to apply for jobs at Petrichor.

III. Would likely invoke FTC Issues
The second issue is that this program would likely invoke FTC action. The FTC is the prime enforcer of privacy in the United States. They punish unfair, and deceptive practices. The creation of Petrichor Face would likely constitute an unfair or deceptive practice.

The FTC will punish corporations who have deceptive or unfair business practice when it comes to the management of users' data. In Petrichor's privacy policy, they state that they protect users' privacy from invasion, and do not share it with anyone without express consent. If they do proceed with the Petrichor Face program, they will be sharing data without the users' consent. Similar to *in re Snapchat*, Petrichor will likely face a complaint from the FTC due to their choice to not comply with their own representations made in their privacy policy, like how Snapchat failed to follow their representations relating to image deletion and location tracking.

Additionally, not following your own privacy policy will make you very untrustworthy to users. This could have significant harms to a corporation that is just beginning to grow, and would definitely impact people's willingness to join. Lastly, this could cause significant problems in expanding into European markets where provisions like the GDPR are generally much stricter than the consumer privacy laws in the United States.

Sample Answer B

Petrichor should proceed with the facial recognition algorithm. However it should not sell to military or law enforcement. There are many ethical and innovative ways to pro12t from facial recognition technology.

For example, cooperating with electric cars for users to identify important contacts, identify potential markets, sell the technology to environmental protection organizations against animal poachers; selling facial recognition to news media for drones in reporting emergencies. Military and law enforcement use is a terrible idea for Petrichor to go through Fourth Amendment & Fifth Amendment hurdles and jeopardize Petrichor's public image.

A. Petrichor should revise Contract Formation of TOS and Privacy Policy language to prevent FTC lawsuits.

Contract formation is faulty. The Petrichor Privacy policy contradicts the TOS. The privacy policy says that Petrichor will not share info with third parties or use data without consent. In contrast, the TOS explicitly requires the user to license generated content "for whatever purpose Petrichor chooses." Before proceeding with the facial recognition algorithm, Petrichor should expressly state the use of data in the privacy policy and make TOS a clickwrap call to action. After a valid contract formation, courts tend to honor the users' licensing. *Sinclair v. Ziff Davis LLC II* (agreeing to Instagram's Terms of Use, Plainti13 authorized Instagram to grant API users, such as Mashable, a sub-license to embed public Instagram content, as set forth in Instagram's Platform Policy.)

Prevent FTC lawsuit. Section 5 of the FTC Act prohibits unfair practices a13ecting commerce. 15 USC §45(a). The FTC applies three basic principles to determine if advertisements are deceptive (1) truthful and not misleading, (2) have evidence to back up (3) whether the advertisements are unfair. Here, the Privacy policy falsely states that Petrichor is not sharing user data with third parties. Petrichor might amass massive amounts of data because consumers trust this description. In fact, Petrichor plans to sell the technology with user data to third parties. Petrichor should amend the privacy policy to prevent deceptive and unfair competition charges.

B. To train the algorithm with photos collected will likely be fair use and no copyright infringement.

Copyright Fair Use. Regardless of the TOS and Privacy Policy, the use of collected data to train the algorithm will qualify for Copyright Fair Use. Users will not be able to sue for Copyright infringement. The court usually consider any one of the four factors outweighing the others to establish fair use: (1) the purpose and character of the use: (a) whether the use serves a nonprofit educational purpose, as opposed to a commercial purpose; and (b) the degree to which the work is a transformative use, as opposed to a merely superseding use, of the copyrighted work. (2) the nature of the copyrighted work; (3) the amount used. (4) the effect on the market.

Here, Petrichor's use of photos to train models (1) satisfies transformative use, because it fundamentally transforms 2D photos to 3D recognition technology. The new cooperation with environmental protection and news media now could satisfy educational purposes. (2) the public photos and videos could be considered facts, and are not necessarily creative works. (3) The nature of the algorithm model requires a

large amount of input data, and compared to other models, the millions of work used might be standard. Additionally, because photos and videos can not be divided, the amount used will usually include the full photo pixel and the full video. (4) there is no competing market effect with the users, since users usually do not sell their photos. The facial recognition is defnitely not competing with the user's own market. Thus, Petrichor satisfied all four factors to qualify for Copyright fair use.

C. The NDA agreement, although well-drafted, needs to consider additional questions on behalf of the employees.

Valid Trade Secret. Petrichor Face will qualify as a valid trade secret, satisfying the six factors: (1) the extent the information is known outside (2) the extent known inside (3) the precautions taken by the holder, (4) the savings e14ected and the value to competitors (5) the amount of e14ort expended in obtaining the information, (6) the amount of time and expense for others to acquire. Petrichor is required to make reasonable e14orts to maintain the secrets, in addition to having the employees sign the NDA.

NDA reasonableness. Three critical questions must be examined: (1) Is the restraint from the employer's standpoint reasonable to protect the legitimate business interest? (2)Is the restraint reasonable not to be unduly harsh and oppressive for the employee to earn a livelihood. (3) Is the restraint reasonable from the standpoint of a sound public policy. Here, the NDA might have public policy concerns.

D. Selling to the military will violate the open source license use code.Then ew cooperation with other organizations will comply with the open-source code.

Conditional License. The open-source license here is similar to permissive license section 2 of the Apache License, where the grant of Copyright License is subject to the terms and conditions of this license. Here, the FreeFlow Foundation's second part of the license forbids "illegal unethical or immoral purposes of use." Selling to the military can violate this condition of the license. Because the military has di14erent national interests and objectives, law enforcement can use facial recognition with bias and racial discrimination. FreeFlow Foundation will routinely require assignments for contributed code, enforce license conditions to secure compliance, and sue Petrichor with strong claims in court for damages as leverage.

E. No violation of Consumer Privacy in Electronic Communications Privacy Act (ECPA)

No ECPA violation, similar to In re DoubleClick Inc. Privacy Litigation. Petrichor quali14es for the ECPA exception. Subsection (a) does not apply concerning conduct authorized or by a user of that service intended for that user; Title II does not apply if a user of an electronic service authorizes someone to access a communication intended for that user. *In re Double Click*. An Internet company does not violate the ECPA's prohibition on unauthorized access to stored electronic communications if the company stores and accesses cookies placed on an Internet user's hard drive. The court said that

DoubleClick is fully authorized to access the full range of information generated by the user.

Here, similar to DoubleClick's access to cookies, Petrichor's third-parties access to user photo data will not violate Title II of ECPA because (1) the photos are likely long term storage on the users' account, and (2) Petrichor authorizes those organizations to access the photo data through Petrichor Face.

Question 5: Global Expansion

Sample Answer A

Another legal issue that may arise as the company expands to more international consumers is one of national security – or at least, the excuse of national security. More security at the cost of privacy is a tradeoff that has been sold to the people of many countries, both new and old, for centuries. And often, the threat of something ominous abroad is the excuse used by governments to invade such privacies. As Petrichor expands outwards, not only will they need to contend with the various security protocols of all the nations in which they intend to operate, but their international expanse will also be used back home by some government officials in an attempt to infiltrate their data sources on users. To combat this, both home and abroad, Petrichor can (and it will be assumed that they already do) employ strong end-to-end encryption.

Encryption ensures the protection of the data and privacy of a particular entity's users. Here, Petrichor users' data will be protected by encrypted code, only accessible to those with a key. This safety measure keeps everyone out, good and bad actors alike. However, government actors, in the name of national security, often pursue obtaining backdoors to these encrypted data sources, in order to combat the protected communications of people like terrorists. And while this is certainly a worthy goal, backdoors don't only let good guys in. Such access opens the way for more hackers and bad actors, such as authoritarian governments who seek to use the protected data to snuff out political dissidents, suppress free expression, and further oppress minorities. Some argue that encryption is the last refuge of criminals, but in some places on the international stage, it is the last refuge of free expression. It's for these reasons that end-to-end encryption is so vital and something that Petrichor should never waiver on.

But abroad is not the only place where Petrichor will face such attacks on encryption. Here, in the United States, they will also face political pressure for the same exact thing, which is exemplified by the 2020 attempt to create an encryption backdoor in the EARN IT Act.

This is important for Petrichor because as a small, growing social media platform looking to expand internationally, they should be viscerally aware of the power that their user-data- collecting capabilities bestow upon them, and the lengths that governments and companies, both abroad and domestic, will go to acquire it. If Petrichor is indeed serious about their public image and cares for their users' data (maybe they aren't

considering their contemplation of the facial recognition software to be sold to military and law enforcement followed by an almost-sarcastic winky-face), then fighting for their own encryption is paramount. They should fight other governments' attempts to access, as well as their own government's attempts here at home, perhaps through lobbying and working alongside technology privacy and electronic rights organizations. However, maybe Petrichor wants to maximize its exposure and profitability as much as possible. Such sentiments are also implicit in the facts. In which case, perhaps being as open and accessible as possible to governments across the globe will be the most fruitful for them, but perhaps a little more ethically questionable.

Sample Answer B

If Petrichor wants to expand globally, they need to be concerned about the impact of the General Data Protection Regulation (GDPR) in the European Union. Privacy is considered a fundamental right in the European Union, and their data protection laws have greater breadth and strength than those in the United States. First, the definition of "personal data" in the GDPR is broad, including "any information relating to an identified or identifiable natural person." This data must be processed "lawfully, fairly and in a transparent manner" and can only be "collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes."

Processing of data is only lawful if there is consent, it is necessary for the performance of a contract, it is necessary for compliance with a legal obligation, it is necessary to protect the vital interests of the data subject, it is necessary for the performance of a task carried out in the public interest, or it is necessary for the purposes of the legitimate interests of the controller.

The GDPR possesses strict conditions for the consent of the data subject and prohibits certain categories of data processing, such as data regarding racial or ethnic origin, political opinions, religion, union membership, and sexual orientation. The data subject can request the data that an entity has on them, request correction of incorrect data, and request erasure of that data.

This is important for Petrichor because, without massive changes to their data collection system, they are open to great liability while operating in the European Union. In order to comply with the GDPR, Petrichor should establish a group to manage the data collection of the company and ensure it is in compliance. Additionally, Petrichor needs to create a much more in-depth and comprehensive user and privacy policy. If it wishes to use any of the data of its users in the European Union, this privacy policy must state what data they will collect, and for what purposes this data will be used. This privacy policy must be presented "in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.