CS 231
Peter McCrea and Nathan Hayes-Rich
Ethics Scenario Analysis #1 -- scenario1.pdf

A. Identify the main ethical question or questions faced by the main character ("you") in the scenario. This will certainly include "what should you do?", but there may be other interesting questions to consider.
    a. **Non-DMCA:**
    The main ethical question is balancing the rights and ethical obligations of all major parties. Would not disclosing this security vulnerability increase the likelihood of millions of people having their private data leaked? (probably yes) Would reporting this security vulnerability lead to you getting swamped in civil lawsuits regardless of their merit? (probably yes given the information in the assignment description) Would reporting this security vulnerability lead to you getting swamped in criminal lawsuits regardless of their merit? (maybe) Does your moral obligation to help keep users' data secure outweigh the cost of potentially rotting in federal prison for decades while simultaneously being bankrupted?
    b. **DMCA:**
    Same as above except you need to worry about whether you're also incriminating yourself by reporting the bug which you had to violate Section 1201 of the Digital Millennium Copyright Act to discover.

B. For each stakeholder (or category of stakeholders) in the scenario, identify the stakeholder's relevant rights.
    a. **Non-DMCA:**
    Users of InstaToonz have the right to assume their personal data and private messages will be protected from outside observers (not necessarily a legal right (unless you and InstaToonz are located somewhere with laws like the GDPR or something like that) and perhaps InstaToonz even had some sort of agreement during their signup process stating that you should not assume private messages would be private. However, the ACM code of conduct strongly implies users should be able to have the reasonable expectation of privacy when using systems like InstaToonz).
    InstaToonz has various legal rights under US law such as the Computer Fraud and Abuse Act and others, which generally criminalizes unauthorized (or initially authorized but later exceeding that authorization) access to computers. Additionally, they have the right to the privacy and protection of their intellectual property and trade secrets, of which, unauthorized access would be in violation of.
    You have the right/obligation (if you subscribe to the ACM's morals) to uphold the public good, prevent harm, respect privacy, and to potentially "access computing and communication resources only when authorized *or when compelled by the*

public good". These rights obviously don't magically counteract laws, however, and may put you in violation of several of them.

b. **DMCA:**
The rights of **users** and **you** do not change, but **InstaToonz** gains additional rights under Section 1201 of the Digital Millennium Copyright Act to not have their encryption and copy-protection circumvented.
Additionally, the **creators** of the copyrighted songs that were supposed to be securely shared over InstaToonz have legal rights under copyright law and Section 1201 of the Digital Millennium Copyright Act, as well as the "ACM right" to assume that the digital platform they allowed their music to be shared on was built by competent engineers who understood security.

C. List any information missing from the scenario that you would like to have to help you make better choices.

DMCA and non-DMCA:

a. Am I able to completely ensure my anonymity? Could all of my security research and communications be done through Tor or using something like Tails? How was my security research conducted? If I reported the bug anonymously, could InstaToonz still somehow identify that I was the one who submitted the report by virtue of forensic investigation of their system?
b. Is there legal precedent for someone who reports a bug like this getting prosecuted and jailed or is their precedent for these cases largely being dismissed?
c. Do I have access to pro-bono or paid legal advice? If so, that changes the equation in the sense that potential legal risks can more accurately be quantified.
d. Do I truly believe disclosing this bug helps the public good? E.g. Are the messages most users share using this service important things like personal information, credit card details, etc or is it all relatively inconsequential information that users wouldn't mind if it went public?
e. Would disclosing this bug have broader impacts than with just InstaToonz? Did I actually discover a huge 0 day exploit that would affect other services, or did InstaToonz just have really bad design?

D. Describe your possible actions, and discuss the likely consequences of those actions.

DMCA and non-DMCA:

a. **Action:** Do nothing.
    i. **Likely Consequences:**
    ii. For **you**, nothing, unless **you** actively use the services provided by InstaToonz, in which case, **you** are at risk for having your information exposed by exploitation of the bug.
    iii. For **InstaToonz**, unless the bug is exploited to reveal users' banking information, or social security numbers, there are no likely consequences. The US government has historically not made efforts to penalize institutions or corporations that fail to properly secure their users' data

(with the recent exception of the Equifax Data Breach, where massive amounts of critical user information was leaked).

iv. For the **users**, there are potentially massive consequences if the bug is exploited and user data is leaked. If passwords, addresses, credit card / banking information, or other critical information is leaked, potentially hundreds of millions of users could have their entire life compromised if malicious entities can coalesce this information and use it to commit identity theft, or credit card fraud, for example. In this case, there's no real difference between the DMCA and non-DMCA cases.

b. **Action:** Attempt responsible (and private) disclosure of the bug to InstaToonz and lawyer up.
   i. **Likely Consequences:**
   ii. For **you**, a potentially life-changing / money-draining lawsuit from InstaToonz to protect their trade secrets. If the bug involves a violation of the DMCA, then **you** potentially face a multi-pronged lawsuit in which you violated InstaToonz' trade secrets and their copy-protection. In either case, InstaToonz is unlikely to drop the lawsuit a second time (especially after reiterating their stance on "security researchers").
   iii. For **InstaToonz**, time and money in issuing and participating in the lawsuit as well as a legal investigation.
   iv. For **users**, nothing, provided that InstaToonz patches the bug before anyone else notices.

c. **Action:** Attempt anonymous (and private) disclosure of the bug to InstaToonz.
   i. **Likely Consequences:**
   ii. For **you**, nothing, provided that **you** can successfully keep your identity anonymous (perhaps by mailing in the bug on a piece of paper, or calling it in from a phone booth). If **you** are unable to hide your identity, then you risk the same consequences of action (b).
   iii. For **InstaToonz**, time and money in participating in a forensic and legal investigation, and potentially a lawsuit if they uncover the identity of the bug-reporter.
   iv. For the **users,** nothing, provided that InstaToonz patches the bug before anyone else notices.

E. Discuss whether the ACM Code of Ethics and Professional Conduct offers any relevant guidance.

DMCA + Non-DMCA:

a. The ACM states that it is **your** right to uphold the public good, prevent harm, respect privacy, and (most pertinently) "access computing and communication resources only when authorized *or when compelled by the public good*."
It seems relatively clear that absent any potential legal consequences, preventing millions of people from having their private data leaked would generally fit the spirit of the unauthorized access exemption in the ACM ethics guidelines.

b. The ACM also makes it clear that **InstaToonz** should have developed their service so that it would be “robustly and usably secure.” Additionally, InstaToonz clearly should not pursue criminal or civil punishments for white hat hackers under the, “Articulate, apply, and support policies and processes that reflect the principles of the Code” section of the ACM. Finally, InstaToonz should “respect privacy” by fixing this issue and being glad that a white hat hacker found it before a malicious user did.
   All in all, it is clear that InstaToonz will be flagrantly violating the letter and the spirit of the ACM Code of Ethics with almost everything they do in this scenario. As stated before, InstaToonz ideally should have developed the application in such a way that ensured user security, developed some sort of bug bounty program or publicly released a statement supporting ethical security vulnerability disclosures, and should not use intimidation or lawsuits to cover up their lack of security.

F. Describe and justify your recommended action, as well as your answers to any other questions you presented in part A.
   a. Keeping in mind the goal of minimizing personal harm from lawsuits, jail, character defamation, etc while maximizing public good from protecting privacy, one of the best options seems to be an anonymous disclosure of the bug to InstaToonz. This method if implemented correctly seems to check all of the relevance boxes. It correctly informs InstaToonz of the bug you found, allows them to fix the bug to ensure user privacy is not compromised, and in theory protects you from any lawsuits if your anonymous reporting method is actually anonymous.
   b. If you have reasons to believe that anonymous disclosure is impossible, you might want to flee to a country that does not extradite to the US if you believe that the public harm from not reporting the bug substantially outweighs the personal harm from reporting it.