Ethical Analysis

Avery Watts, Ben Aoki-Sherwood, Kenyon Nystrom

A. The ethical dilemma we are faced with is whether or not to report the bug to InstaToonz--or possibly, to report it to a more trusted third party like the FBI or some other government agency because of the threat of retaliation by InstaToonz. Clearly, we have an ethical imperative to make InstaToonz aware of the bug so that they can fix it and protect their customers' privacy. However, this imperative is tempered by the knowledge that we could be sued by InstaToonz and maybe even be accused of trying to steal trade secrets. Another ethical question is what should we do and what *can* we do to try to make InstaToonz more security-friendly. They have already pushed back on calls that they start a bug bounty program, which is a proven way that many large corporations catch bugs. In light of this, do we push them harder to look for bugs and security vulnerabilities? If so, how? This and the previous question become more complicated if the bug involves the encryption or copy-protection of the music, because then InstaToonz has solid legal footing to try to prosecute us under the DMCA for unearthing the bug, since our knowledge of the bug is a circumvention of their rights controls.
B. The users of InstaToonz have the right to privacy; they have the right to not suffer "unjustified disclosure of information", as the ACM Code of Ethics states. If this bug involves copy-protection or encryption of the music shared by their users and we are in the US, then InstaToonz has the right to prevent circumvention of their access controls under Section 1201 of the DMCA, which means they would have the right to sue us and probably fine us or throw us in jail. If we are not in the US or the bug is unrelated to copyright or encryption, then they do not have the right to punish us this way, at least under the DMCA. We are also a stakeholder in this situation; however, it seems like we don't have many rights here, especially if InstaToonz can trample all over us with the DMCA. We have some nominal "freedom of speech" if we are in the US, but it seems like disclosure of this bug would count as circumvention of access controls and thus not be protected speech, so the 1st Amendment probably doesn't help us much. However, maybe if we got in touch with InstaToonz in private we could maybe make the case that our intent was not to circumvent the encryption of their music but to actually prevent future circumvention by malicious parties.
C. Information missing:
    a. Does InstaToonz have some sort of user privacy statement which guarantees that users' private conversations will not be shared with anyone?
    b. To discover the bug, did I have to gain access to an encryption key or bank of keys that would allow me to decrypt music on InstaToonz? This would only be particularly pertinent in America.
    c. Are the actions we took to discover this bug relatively effortless in the grand scheme of intrusion? i.e. is it reasonable to believe that the bug has already been

or likely will be soon discovered by an average infiltrator with potentially malicious intent?

d. To what degree did the calls for boycott/congressional action gain traction? With enough public backlash, one is more likely to avoid direct confrontation/suits for fear of the potential damage to the use of the social media platform.
e. What lawsuits specifically did InstaToonz bring upon the last person to report a bug? To what laws and protections did that threat pertain?

D. Courses of Action:

a. Find some way to anonymously report the bug to InstaToonz. It would be possible to contact their offices or customer service through a public phone or from a throwaway email address. The downside of reporting the bug this way is the possibility that a phone call or email on this subject would not be taken seriously. Since this is anonymous, even if the law was broken, there wouldn't be consequences.
b. It would also be possible to anonymously post the bug online where InstaToonz would see it. An anonymous Medium post would be a possible route to report the bug to the public. The downside of such action is the possibility the bug would fall into the wrong hands and be used by malicious actors. Assuming the website on which the bug was posted keeps the personal information of the poster anonymous, even if the law was broken, there wouldn't be consequences.
c. Bugs can be reported to the U.S. government through intelligence agencies, such as the FBI, NSA, CISA. It is possible to report a bug to CISA through a link on this website: https://us-cert.cisa.gov/report. If the finder of the bug broke the DMCA, there is a possibility the law enforcement agency to which the bug was reported could find the reporter in violation of the law and prosecute them.
d. Bugs can also be reported to private security firms, such as FireEye, Kaspersky Labs (although they're Russian), or CrowdStrike. However, there is no guarantee these firms would report the bug to InstaToonz. These firms would have the knowledge to handle reporting the bug if it is in violation of the DMCA.
e. It would be possible to leak knowledge of the bug to cyber security reporters. Reporters and their news organization would have a greater range of freedom of speech and would better know how to handle a possible breach of the DMCA.
f. A security researcher could take the aggressive step of anonymously hacking them using the bug and make their presence known, but without stealing any information. This would be breaking the law, but not necessarily be morally wrong. If the security researcher is caught, they would likely go to jail, regardless of their arguably correct moral reasoning for hacking InstaToonz.
g. Another aggressive step an experienced white hat hacker could take if they're confident in their own anonymity is to threaten the company by bluffing to release the hack unless the company fixes the bug.

h. A security researcher could publicly report the bug and hope for public backlash. If the security researcher doesn't think they were in violation of the DMCA, this route would become significantly easier. There would be relatively little for which InstaToonz could sue you. However, even if the bug was in violation of the law, calls for boycott or congressional action could reduce the chances of the security researcher being sued. There is a chance further public outcry would convince InstaToonz to create a process for reporting bugs, such as a bug bounty program.
i. Do nothing, since reporting the bug may result in a lawsuit or being found in violation of the DMCA, and hope their security team finds the bug before malicious actors do. Since InstaToonz is against other people finding bugs on their platform, let them find their own bugs.

E. As mentioned previously, the ACM Code says that our actions should serve to "avoid harm"--in particular, we should avoid "unjustified disclosure of information", which is what would happen if we or anybody else exploited this bug to access the InstaToonz users' DMs. The Code also tells us to "respect privacy" and "honor confidentiality". The former suggests that we need to work to get the bug fixed somehow to ensure that the users' data remains private. The latter complicates our course of action, because the knowledge of this bug could be considered confidential information belonging to InstaToonz, so disclosing to some third party trusted authority could be a violation of confidentiality. This is related to the DMCA; under the DMCA, any sharing of this bug could be construed as circumvention. However, the Code indicates that if confidentiality violates the Code itself, information should be disclosed to the appropriate authorities. This seems to apply in this case, as keeping the information secret could result in a violation of privacy for InstaToonz users. Again, though, this butts up against the restrictions of the DMCA if the bug involves access controls.
F. We recommend anonymously reporting the bug to both InstaToonz and the relevant authorities, i.e. CISA. Unquestionably, we need to make the existence of this bug known to InstaToonz so that they can fix it and protect their users' data. However, we also don't want to be sued or imprisoned for our whistleblowing, hence the anonymity and the reporting to both authorities so that the government can back us up and confirm that our intentions were not malicious in exposing the bug. If the bug does not involve encryption and copy-protection of InstaToonz's music, then we can be more confident in giving this information to the government, perhaps even showing them how the vulnerability works, as we would not need to be as afraid of being punished for circumvention.
    a. Question from A: do we push InstaToonz harder to look for bugs and security vulnerabilities? If so, how?
    Answer: it is our ethical responsibility to do so, because their practice of vilifying security researchers and not using bug bounties is clearly jeopardizing the rights of their users. However, based on their confrontational history, the best way to encourage them to do so would be to use the existence of this bug to push

government agencies or even Congress to hold hearings and possibly consider regulations that would force InstaToonz to update their security practices.