

The main ethical question in this scenario is that how I should report the bug to InstaToonz so that the security loophole can be fixed, the public can learn about this issue, and I will not get myself into trouble. If this scenario takes place in the US, I need to be careful not to decrypt or copy any music product shared by InstaToonz users, and I definitely should not reveal to anyone about the bug before communicating with the company. However, if it involves encryption or copy-protection, I need to be hesitant to directly report to the company, in case they think I have already violated the anti-circumvention law when discovering the bug.

There are three main categories of stakeholders in this scenario: InstaToonz, the public/users, and I. InstaToonz has rights over the security of the company's products and information. The users have the rights over the security of their private messages, and the public have the right to learn about this security issue for making future decisions on using InstaToonz products. I have the right to request engagement in the bug bounty program, and if requirements are met, I have the right to get payment as described in the program's policy. If encryption or copy-protection is involved, the company also has the right that music shared on its platform not being decrypted or copied by anyone.

In order to make better choices, I also need to know the detailed policies of the bug bounty program: how much can I get paid, and if I can disclose this scenario to public after the bug is fixed. I would also like to know if the company can sue me for their loss due to my disclosure of the bug, and if the company is likely to win. It is also

important for me to know whether the bug involves encryption or copy-protection, and if so, whether I have violated the anti-circumvention law by discovering the bug.

I can make these possible actions:

1. Directly report to InstaToonz privately and ask for enrollment in the bug bounty program. This may earn me a payment, but the company may sue me like they did to someone before. They may also try to stop me from disclosing the bug to public even after it is fixed to protect its reputation.
2. Not report to the company or disclose to the public. I will not face the risk of being sued, but it is unethical to do so, because hackers may find this bug too and maliciously exploit it.
3. Anonymously report to the company and then anonymously disclose it to public after it is fixed. I will not earn a payment, but I do not face the risk of being sued, and the company can fix the bug to protect the customers. The public can also learn about it later on, but they may not think it is reliable since I do it anonymously.
4. I can let someone trustworthy to learn about the bug, and let this person report to InstaToonz. I can then step away from the risks, but that person may be in trouble. Also, if the bug involves encryption or copy-protection, I will violate the anti-circumvention law by telling someone how to circumvent the technological barriers

The ACM Code of Ethics and Professional Conduct says it is a professional responsibility to “Foster public awareness and understanding of computing, related technologies, and their consequences.”, so I should disclose the bug to public after it is fixed to raise awareness about information security and the risks of technology. It also emphasizes the respect for privacy and confidentiality, so I should not decrypt or copy any music or private messages through the bug, nor should I tell anyone about it before it is fixed, whether this involves encryption or copy-protection or not.

Due to these reasons, I recommend first to consult a lawyer about the anti-circumvention issue, and then to anonymously report the bug to the company and then anonymously disclose to the public while not decrypt or copy anything using the bug. In this way, I can protect myself from unwanted trouble but also fulfill ethical responsibilities, while the only loss is the potential payment from the bug bounty program, solving all the questions in part A.