a) Should I report the bug and possibly be sued, arrested, deported and be in serious financial debt from the legal fees? Should I not report the bug, letting it remain in the system, potentially affect thousands of users? Will the company effectively acknowledge my claim? Will the company fix the bug if they acknowledge my claim? Can the company find the bug independently if I don't report it? How long will the company take to fix the bug, if they choose to do so? Does the public report of the bug affect the company's trust in the market and its trust among its user base? if so by how much? Will the disclosure of the bug make the company's stock go down? If so by how much? How much money will the company lose if the bug is publicly disclosed? How many people are affected by the bug? How bad is the bug for the people involved? What do the people involved have to lose if hackers exploit the bug? What do people talk about in their messages? What type of information is shared in private messages? Do people share private and/or sensitive information in their private messages? Can the messages be connected to their profile? Can the data shared in private messages be connected to the people? Is data mining or monitoring by the company (or a third party) done in private messaging? If I decide to disclose the bug, will the company sue me like last time (even after the bad PR)? Did the company change its view towards people who report bugs? If sued, do I have a chance to lose provided on how the previous lawsuit turned out? Will the second lawsuit follow a similar path? Did the company do any lobbying in the meantime to get the legal side in a more advantageous position from their perspective? How hard is the bug to find? Has anyone exposed it before, or found a similar issue? If a similar issue has been found, has it been addressed? Is there a report bug section in the app? Can I report the bug anonymously? Can a bug report, maybe on a public computer, not be tied to my identity? Will this jeopardize my hiring prospects at this and other companies if I leak the case becomes a cause celebre?

b) **Artists:** The right to have the copyright on their music, the right to make money on it, guarantees that it will not be pirated and illegally distributed. Freedom of expression (they are allowed to post their art on the website without backlash), the right to encryption and private communication.
Record labels: The right to distribute records on behalf of artists, the right to artists names and music, the right to copyright music, the right to post it on different platforms, the right to make money on it, guarantees it will not be pirated or illegally downloaded, the right to negortiate contracts with artists and websites like the company.
Users: Right to privacy and secret messages, the right to buy and/or stream music on the app, right to have their secret information protected, right to be safe from fraud. Right to talk to other users/artists without a third party reading their messages, data rights (in terms of data mining), the rights assured by the terms of use and privacy of the website, they have the right to their financial and credit card information as well as the right to keep their sensitive information secret.
Company: Rights over the system, algorithms, server, and platform. They have the rights over the techniques they used to build it, as well as the projects they have, as long as they are copyrighted. They have the right to their terms of use and privacy, as long as it complies with the federal, state, and local laws. The rights to their cookies, data managing, and information collecting mechanisms. The right to track their users. The

right to keep their trade secrets secret, the rights granted by copyright, the rights granted by the DMCA, the rights of what they created and developed for the company.

Company and the **Local government:** it will probably will not care about the system or it will be out of its jurisdiction. But the company has to follow the laws of whatever city/county it is based in, and the system probably has to comply with local laws of the place the user is accessing it in. If it is being accessed in Memphis, TN it must comply with Memphis laws. The local authorities have the right to pass laws and collect taxes from the company, and all its users.

Company and the **State Government:** Might care about the system. The company must comply with state laws. They might differ, for example California privacy laws and Minnesota privacy laws might be different. It also has to comply with laws based on where it is being accessed in. The state has the right to collect taxes, and approve laws. The company has the right to sue users and the state has to provide them with a fair trial. Charges might be dropped and the state has the right to stop the investigation.

Company and the **Federal government:** The company has to abide to federal laws, including to the DMCA, and copyright laws. The government has the right to collect taxes and pass laws to regulate the company. The company has the right to sue users and the federal government has to provide them with a fair trial. Charges might be dropped and the investigation might be frozen/stopped.

Me: The right to use the system in a way that complies to the terms of use and privacy policy. The right to use the system as long as I do not breach the DMCA laws, or try to crack and expose private algorithms, know hows and techniques used in the system, the right to buy and maybe stream music on the service, the right to have my personal information private, the right to my sensitive data including but not limited to my banking information.

c) Why did I find the flaw in the first place, did I just stumble upon it while using the service? Did I dig into copyrighted material, that is protected under DMCA or other copyright laws? Did I try to tamper with algorithms, or private encryption algorithms? Did I tamper with what was created with the system creators? Is the bug hard to find (i.e. are hackers likely to find it and exploit it)? What is my financial status (If sued do I have money to pay for all the lawyers and legal fees)? What is my immigration status (Can I be deported as a result of the legal battle)? What is the possible fine that I get? Can I get jail time for exploiting the breach? What are my odds of winning the lawsuit? If found guilty do I have the means to pay the fine and would be willing to serve the jail time? What is my job (if I work for their competitors, I am likely to suffer a more severe consequence, as they might accuse me of industrial espionage)? Do I have a team or a company behind me to expose the flaw in their system? Do I work for the company I found the bug in the system (if so it is easier to disclosure it)? If I am an artist, how much money do I lose in this scenario that my copyrights are violated based on the bug I found? Do I have information in the system that I wouldn't want it to be leaked, if so will this bug leak it? What type of information do I share on private messages? Will this issue put regular

users in financial trouble? What type of content is shared in those private messages? Do artists communicate and negotiate record label contracts in them? If so, what type of things do users say in these messages? If they are leaked, what is the worst that can happen (regular users being frustrated or revealing sensitive information like addresses and credit card numbers)? What other form of media, in addition to music is shared on the platform? Is that media shared via chat? Do people share sensitive or private information like credit card numbers or documents on these private messages? Can this bug lead to access in other areas of the system? Can other information in this database be subject to being exploited by a similar bug or the same bug? Does this bug indicate other bugs that might be in the system? How serious are these other bugs? Is it possible to link the information on the system to any particular user? Is it possible to use it to steal information from artists, like record deal details, or steal new songs? If so what can be leaked? Will the company fix the bug? How long will it take for the company to fix the bug? Has the company changed its policy based on the results of their previous lawsuit?

d) Report the bug: There are a few consequences to this action. The best case is that the company thanks me and fixes the bug. The second case is that the company sues me and fixes the bug. The third case is that the company sues me and does not fix the bug. In case the bug goes public (regardless of whether the company sues me or not) the market will lose part of the trust they have in the company. Their shares will drop and they will lose money, people might be fired as a result. It will be really bad for PR, people dislike having their personal messages leaked. Many users would stop using the site and migrate to a platform with better privacy. If the company sues me and does not fix the bug it will be even worse for their PR. Security professionals will probably take my side and there will be vehement opposition to the company's actions. Users and artists might dislike the actions of the company, that is not improving their system when bugs are reported. This might lead to rumors that the company does not care about their user's privacy, which is also bad for PR. Users will stop using the system, people will trust them less, stocks will drop and less money will be made. If they sue me and fix the bug, they will show that they care about the system by fixing the bug. However, this is also bad PR because instead of thanking those who want the system to be better the company would be suing them. Security professionals will backlash the company, and users will be not happy about it, as it was a bug report. This will be divisive though, those who approve the copyright laws and the DMCA might take the company's side. The company will be in the media because of the lawsuit which is bad for their image and reputation.
Do not report the bug: users might have their messages leaked and exposed. It might be sold to hackers or scammers. If they share private information in their messages it will be available to whoever exploits the bug. The worst part is if their financial information is leaked. In this case, people might go bankrupt and their money might be recklessly spent online. Their sensitive information (if they share it via message) might also be publicly available online, which might lead to identity theft and fraud. For artists and record labels, if they share song ideas and contracts, this sensitive information might get leaked. Private information about artists' revenue and contracts will be made public. If they share audio online (and/or lyrics), people might steal their song ideas, and record it themselves. In the worst case they might even make it their own intellectual property.

Secret information about artists like album information or new song information might be released ahead of schedule. If record labels and artists, or artists and the system share files, unreleased songs might be leaked. They might also be subject to piracy and have their songs illegally streamed and owned by other people. Messages between users and the artists might be disclosed, which leads to gossip and speculation. There might be more bugs in the system which have a similar cause. These bugs might be exploited by hackers.

e) The code has many sections which indicate (or at least imply) that the bug should be reported, such as the one which says “Avoid harm.” People might suffer harassment from scammers if their data is leaked, people might get financial consequences if their banking information is leaked, and be subject to physical threats if their addresses are leaked. Such information might be present in private messages. This section also mentions unjustified disclosure of information, which, in this case would be the result of a data leak. It also says that a computing professional has an obligation to report any signs of the system that might result in harm.
Another section that suggests me to report the bug is under “Respect privacy” part. The system issue might enable the collection, monitoring, and exchange of personal information that should remain private. In this case, the system also does not honor confidentiality, as it is exposing client data. So, for the code to comply to it, I should report the bug.
Last but not least the section that says“Design and implement systems that are robustly and usable secure.” is violated. As the system is not secure. There is a bug that might make all the communication in the site public. So to help the code uphold these standards I should report it to the company.
The code also has sections that indicate that the bug should not be reported. For example, “Strive to achieve high quality in both the processes and products of professional work,” as the company does not have a bug bounty program and does not receive bug reports well they are not supporting high-quality work from their professionals, and do not value the dignity of their clients and users. They are refusing feedback from users that might help their system.
Most prominently “Accept and provide appropriate feedback,” in this case. is clearly violated. When they received a critic last time they decided to sue the person who made it. The code also outlines that one should “give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks." In this case, as the company does not give value to public testimony from users and responds with backlash, so this section is being violated.
While the ACM Code of Ethics provides an excellent background and a good framework for thinking, a great part of its measures have to be implemented primarily inside the company. There are measures that cannot be implemented or requested by system users, such as “Strive to achieve high quality in both the process and products of professional work.” Most measures described, like the process of developing software should be implemented by a team. What is more, the company is violating multiple principles of the code, not only because it is not secure, but also because of the way they respond to responsible disclosure. If I were to act according to the code, I would

disclose the bugs, but as the company is not following the code they might have a hostile response. In a scenario where everyone is following the code, or doing their best to do it, then disclosing is the way to go. But in a situation where people are not, then you might get into legal and personal problems by following the code.

f) I would not disclose the bug. The company might sue me and I do not want the headache of being sued, going through a long trial, and facing the possibility of jail, deportation, and being in debt because of legal fees. In addition to that there is a hefty fine for violating digital copyrights in the DMCA. The bug in this case will remain in the system unless the company finds it or somebody else reports it.
Based on the way the company dealt with their previous bug report, I do think they will acknowledge my claim, but instead of fixing the bug right away, they will sue me first. If the bug is leaked, the bad publicity might force them to fix the bug, so I do believe that the bug will end up being fixed.
As the bug is in the system, and was found by a regular user (me), I strongly believe it can be found independently by the company. I assume I did not intentionally try to crack their code, algorithms, private encryption, or know-how, nor used the system in a way to break it. So, as a regular user, while browsing the system found the error, the developers are likely to find it too. By my assumption, however, the bug involves the encryption and copy-protection of the music shared by the users so it is protected by copyright.
I do not know how long the company would take to find and fix the bug, I do not have access to their system, or their code, nor know what caused the bug. I do not know what needs to be done to fix the bug, nor how long it will take to implement it. Only the engineers in the company know what is going on and cam estimate the time it will take to fix the bug. It also depends on whether the bug fix is prioritized or not.
This is quite a serious bug, so it will certainly make the market and the users trust the company way less. They might lose users right when the bug is first disclosed, especially those who are particularly careful about the disclosure of their information. Some artists will flee the company as they do not want their private messages leaked and to become gossip on websites. The record labels might be afraid of their private messages being leaked and they might have concerns about their copyrighted material, so they might leave the site. All of this makes the market trust them less, as the system is not secure. I don’t know how to estimate the number of users, artists, and record labels that would stop using the app. This will cause their stock to go down. Again I don’t know by how much because I do not understand the stock market well. But I think the shares will fall quite a bit. While I know that the company might lose a lot of money if the bug is disclosed, I don’t know the exact amount. Probably millions, I also don’t know their revenue to estimate how bad this would be.
Thousands of people are affected by the bug as mentioned in the assignment. I believe the bug is quite bad for the company and artists, but not so much for regular users. I doubt they share personal or private information on a site that focuses on music. I do not believe people share their credit card information or sensitive information, they are also unlikely to share their address. I believe that the most sensitive information they might share is concert tickets or their zip codes (city they live in, area they are at). The tickets might be stolen, but most concerts aren’t extremely expensive. I also think that the

dialogue is mostly between regular users or users and artists they like. The content of the messages is most likely about music, concerts, and LPs. While it is bad to have that information leaked, it is not very important information, and while it might be harmful it is not that harmful. The information might be sold to scammers, which is pretty bad. Scammers might try to trick people which is really bad. Overall it is a serious bug for clients, but not the worst possible. If artists talk among each other, or with record labels, more sensitive information might be shared. This would be really bad for them. Hackers might steal and copyright song ideas from artists and disclose their contracts with record labels. Secret information/communication between artists and record labels might be disclosed, so they are likely to loose a lot of money. For them, the bug is very serious.
I believe that the messages can be connected to the person or artist/record label, which is pretty bad. Especially if they use first names in communications. So, the data can be easily matched to their profile and to the people themselves which makes it quite a serious bug.
The company might not do monitoring/data mining in private communications. However, I don't know for certain, as I do not know their terms of use and privacy policy, nor know the data policy of the country or any of its states. This might be illegal, or at least illegal in many places. I do think selling messages to third parties is illegal.
I do think that the company would sue me. Even after the bug reporter got the upper hand in the previous lawsuit, the company did not change how it thinks. They still put security researchers in quotes, and say they are trying to steal information from them. They also do not have a bug bounty program. Based on their actions, they did not change their thoughts on people who report bugs to them. If sued, I think I not would win the lawsuit as it happened in the previous case. I did violate the DMCA, and the penalty is a fine plus jail time. I did not do so intentionally, but I don't know whether the court would acquit me. So I think the second lawsuit might result in jail time.
I do not know whether the company did lobbying to change the laws for them to be more favorable to them. I don't know how hard lobbying is, nor how much it costs. But the copyright laws are already pretty extreme, so they can sue people from that.
I do not think that the bug is extremely hard to find, as I assume I was not trying to crack the code, nor forced my way to break the system. I just stumbled upon it. So, I do believe other users (and hackers) have already found it. This is bad, for users and artists.
I do not think a similar bug was ever found. Otherwise, the company would have been more careful before this coding this bug into the system. So I assume a similar bug has not been corrected as well.
I do not think there is a report bug button in the app, as the company does not take bug reports well, and does not have a bug bounty program.
There might be ways for me to report the bug anonymously, maybe through a public computer, VPN and fake email address. I might also try to connect with friends who work at the company to privately disclose the bug. If employees reported it, they are unlikely to suffer backlash. That might be the best course of action, and on second thought I might do it, if I have the means. So, I would not disclose to the company, but to someone who is able to fix it.

Arthur Viegas Eguia

I do not think reporting the bug would jeopardize my hiring prospects at big companies, or companies that have a bug bounty program. However, it might jeopardize my hiring prospects for small companies, or companies that think in a similar way to this one. Still I do not want to go to jail, or have to pay a fine. So my main course of action is looking for a good friend in the company who might fix the bug from the inside, but not disclose it.