Miles Hoene-Langdon

Scenario #1: responsible reporting of security vulnerabilities

In this scenario, the main ethical questions faced by me are as follows. Is it more important to follow the law or follow what I believe is morally right? Does the potential vulnerability of InstaToonz users caused by the bug outweigh my personal vulnerability brought on by disclosing the bug? Do I hold some of the blame if InstaToonz users end up being exploited by the bug and I don't disclose it? Does a legal system against coordinated vulnerability disclosure justify or excuse me from failing to disclose the vulnerability?

The main stakeholders in this situation are the company InstaToonz, myself, and users of InstaToonz. The rights of the company InstaToonz are to keep their trade secrets secret. They developed that app and own rights to it and its design. They don't want people poking around and discovering these trade secrets that they have invested time and money into and that help them generate revenue. The rights of myself are to be able to enact my social responsibility of helping others, without facing unreasonable consequences. I should be able to help preserve other's peace of mind without facing infringement to my own peace of mind. The rights of the users of InstaToonz are privacy and security. They have the right to have their private messages kept private and have good security measures that give them a sense of safety in making this privacy feasible.

In order to make the best possible choice, further information regarding this scenario is necessary. I would like to know the specific details of InstaToonz privacy policy for their users. Also, I'd like to know more about the security bug found by the bug-reporter in North Carolina, so I can see how it compares to the bug I've discovered. It would also be helpful to know the details of the FBI report on the previous matter and the insights of the bug-reporter themself in regards to their situation.

Now, we will examine what the possible consequences are of taking different actions in this scenario. One action in this scenario would be to keep quiet and not attempt to disclose this bug to InstaToonz. The consequence of this action is that InstaToonz users' data is at risk. In the future, there could be a data breach where the personal information of InstaToonz users is exposed using the vulnerability I found. This then causes me to feel guilty. I could have prevented this disaster if only I would have reported the bug. If it was the case that the bug involves the encryption and copy-protection of the music shared by InstaToonz users and I suspect the bug could violate Section 1201 of the Digital Millennium Copyright Act, then I could partially dissociate from the blame. I could consider my lack of disclosure a fault of the system of law and not my own. On the other hand, if potentially violating Section 1201 of the Digital Millennium Copyright Act (DMCA), then it would be more difficult to disassociate. I would directly carry personal blame.

The other possible action in this scenario would be disclosing the bug. Doing this would be personally fulfilling as I would feel that I fulfilled my moral duty and helped others when I

was able. Unfortunately, there are consequences. Based on their past, InstaToonz would likely provide legal pushback against me. This is especially the case if I am potentially violating Section 1201 of the DMCA. It would be helpful to know whether or not in the previous situation, the bug reporter had violated Section 1201 of the DMCA. If I did violate this law it would cost me a lot of time and money with legal fees and hearings. I also could potentially be found guilty and face the worst case scenario. On the other hand, if there is no potential violation of Section 201 of the DMCA, then the possibility of legal troubles is diminished. Although given InstaToonz's statement about security researchers engaging in attempted thievery of trade secrets, InstaToonz would still likely attempt to go after me in some way. Time and money would still be lost, but it is less likely that I would actually be found guilty of anything.

The ACM Code of Ethics and Professional Conduct is helpful in this situation. By disclosing the vulnerability that I have uncovered I am upholding my obligation as a computing professional by minimizing negative consequences of InstaToonz's app that threatens the privacy of its users. Also, the ACM Code states that if a computing professional violates a rule because it is unethical, then they must still take full responsibility for that action. Thus, if I face legal trouble I must be ready and have fully considered what I am up against beforehand. Therefore, by The ACM Code of Ethics, it seems that disclosing the vulnerability, taking responsibility, and being prepared for a legal battle is what I should do.

My recommended action in this scenario is to privately disclose the vulnerability to InstaToonz and prepare for a legal battle. I, the security analyst, must put my fear of legal troubles behind me and do what is necessary to protect the users' of InstaToonz's privacy. If it is the case that my vulnerability violates Section 1201 of the DMCA, then I will break the law knowing the possibility of being found guilty. If I am found guilty under this law, then hopefully it could shed light on the unethical nature of the law and help create a push towards reform. My personal expense could help change the law to ensure that many more in my situation can do the right thing.

I will now answer my questions stated at the beginning in reverse order. First, a legal system against coordinated vulnerability disclosure does not justify or excuse me failing to disclose the vulnerability. As a security analyst I should help change the system by violating the laws and demonstrating, in what happens to myself, that they are unjust. Next, I do hold some of the blame if InstaToonz users end up being exploited by the bug and I don't disclose it. Not disclosing the bug is not holding up to the standards of a security analyst. It would be violating the ACM code of ethics as I would not minimize harm with my actions. The collective potential for harm of the users would outweigh my own potential for legal harm. Who knows what kind of personal information, from the users, could be exposed by the vulnerability being exploited. Helping reduce the damage and worry that it could bring about by others is the selfless and morally just thing to do. Furthermore, ethical laws are put into place to ensure that harm is reduced in society and that the rights of all people under the law are able to be equally expressed. Any law that doesn't uphold this purpose is in immediate need for revision and public push back. It is my moral obligation to contribute to my society and make sure this happens. By breaking

the law in pursuit of what I believe is morally right, I highlight the unethical nature of the law by being unjustly punished. It is crucial that awareness is spread about unethical laws like Section 1201 of the DMCA. This is the only way unjust laws are changed.