# Scenario1

## Eric Neidhart, Ginnie White, Ankit Sanghi

The main ethical questions in these scenario are: what you should do with the bug information now that you have it, if you should prioritize your own time, financial resources, and legal liability over the privacy of InstaToonz's hundreds of millions of users, along with who besides InstaToonz you can/should communicate this information to. Part of weighing this decision is whether or not the relevant vulnerability relates to encryption and copy-protection, and if it is, whether exposing vulnerabilities to the company in question falls under "Fair Use."

In this scenario, the stakeholders in question are you, InstaToonz the company, InstaToonz's users and potentially law enforcement agencies like the FBI. The users have a right to privacy, you have the right to due process if law enforcement becomes involved in the issue as well as "fair use" of InstaToonz's software, and InstaToonz has the right to their intellectual property along with the right to not be hacked under the DMCA.

One piece of information that could be useful in this scenario is whether you know anyone who actually works at InstaToonz who could possibly raise the issue internally, since there is no bug bounty program. That way, you limit personal contact with InstaToonz and thus your personal risk, while having the issue raised from within may cause them to actually take action to fix the problem. Some more information that would be helpful is whether or not the relevant bug was in any piece of the code likely to be covered by Section 1201 of the DMCA, as if it was outside the scope of that section, there is significantly less risk in simply approaching InstaToonz (they may still sue you, but the risk of criminal charges is substantially reduced).

You have several possible options in this scenario. First, you can ignore your findings and do nothing. This would be the easiest option for you, since it costs you nothing and there's always the chance that InstaToonz will find and fix the bug themselves. However, if no one at InstaToonz discovers the bug and a malicious hacker takes advantage of it, you run the risk that doing nothing will lead to a massive privacy breach that affects users and possibly leads to financial repercussions for InstaToonz itself (if now no one wants to use their app, or they have to pay for damages). Second, you can go directly to InstaToonz with your knowledge. If the bug relates to the DMCA, you may find yourself on the receiving end of a lawsuit and a media frenzy. As mentioned with the last person who tried the bug report, this is a massive use of both your time and money; however, if InstaToonz can fix the bug, you may have averted a large-scale privacy breach for many users and save a lot of people harm in the future. If the bug does not relate to the DMCA, you may not be on the receiving end of legal repercussions, even if InstaToonz doesn't thank you for finding the bug. Finally, you can attempt to take your findings to a third party, perhaps another security company or the news. If the story is broken anonymously or comes from a dedicated security company, you may avoid any potential lawsuits yourself. However, you would have to go to an entity that you trusted, and going to more people increases the likelihood that a malicious person will learn of the bug and exploit it.

Section 3.1 of the ACM's Code of Ethics states to "ensure that the public good is the central concern during all professional computing work". In theory, the "public good" in this scenario means protecting the rights of InstaToonz's hundreds of millions of users; they deserve to have their direct messages and other personal information remain secret. This principle suggests that you have a duty to report the bug in one for or another. Section 2.5 says "give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks. In this case, the "possible risks" include the bug you found in the app, and the code implies you have a duty to provide a "comprehensive and thorough evaluation" of this to either InstaToonz or a different entity. Finally, Section 2.8 says to "access computing and communication resources only when authorized or when compelled by the public good". Here, one can argue either that you were not authorized to deal with encryption and copy-protection bugs (if applicable) and thus should not have done so, or that this bug regardless of its DMCA status consisted of a threat to the "public good" of the users and thus needed examining.

We recommend that if you have an inside contact, tell them privately so that they can raise the issue internally and hopefully get the bug fixed. If you don't (or there is no action taken by InstaToonz), then you as a security researcher probably know someone in a security company, and you could reach out to them and let them know. They would then reach out to InstaToonz and tell them about the bug, and InstaToonz will hopefully be more responsive to that. If all else fails, report the bug to InstaToonz yourself. If the bug is not related to Section 1201 of the DMCA, your chances of any legal case falling through are better; if it does relate to encryption and copy-protection, you likely need to prepare to argue that your actions were justified in spite of the act. You may bring up the previous security researcher sued by them in court as a case study. We think that you should probably try and protect yourself throughout this process as best you can, but ultimately, you do have a duty to try and ensure the overall public good even if it costs you.