Ben Hafner
CS 338 Computer Security
May 2022
Ethical Analysis Assignment (Scenario #1)

Part A: Identify the main ethical question or questions faced by the main character ("you") in the scenario. This will certainly include "what should you do?", but there may be other interesting questions to consider.

The main question you face here is whether to share the bug you've found. If you do choose to share it, how and with whom?

More generally, I think the problem at the bottom of this scenario is about how companies should handle security bugs being discovered by independent third parties.

Part B: For each stakeholder (or category of stakeholders) in the scenario, identify the stakeholder's relevant rights.

InstaToonz's users have the right to privacy of their direct messages.

InstaToonz has the right to control and profit from their propriety trade secrets, business model, creative content, and code. If any of this is copyright protected, then this right has legal backing in the United States.

You, as a human being, have the right to not be harassed for discovering a bug. If anything, you should be commended for trying to help InstaToonz patch up their security holes!

Artists have a right to their songs, but I don't think this is very relevant because the security bug compromises private user messages, not songs. Unless songs can be included in private user messages…

Part C: List any information missing from the scenario that you would like to have to help you make better choices.

I'd like to know how quickly InstaToonz would be able to patch the vulnerability if you shared it with them. Also, I'd like to know how quickly a hacker would be able to write an exploit and gain access to user data if they heard about this bug. If the bug is easy to patch and hard to exploit, it might make more sense to share it publicly. On the other hand, if the bug is easy to exploit and hard to patch, you definitely shouldn't share it publicly.

Part D: Describe your possible actions, and discuss the likely consequences of those actions.

One possibility is to report the bug privately to InstaToonz, as is standard practice when a security vulnerability is discovered. Typically, you would give InstaToonz some period of time like a couple weeks to patch the bug before sharing the vulnerability publicly. That way, users' private direct messages data would never be at risk (at least in theory). However, the scenario states that the last time someone attempted to report a bug to InstaToonz in this way, the company retaliated against the reporter with a lawsuit, so you must be prepared to weather the onslaught of InstaToonz's wrath.

Another possibility is to report the bug anonymously. This way, InstaToonz can't sue you. But there are several downsides of this approach. First, you put user data at risk because a bad

actor may be able to develop an exploit based on the bug before InstaToonz has time to patch it. Second, if the bug has anything to do with circumventing digital protections of copyrighted material, you may have just committed a crime by publicly dispersing the tools/knowledge required to infringe on copyrights. Then the government would come after you, which you definitely don't want.

A third possibility is to simply keep the bug a secret. If you don't share the bug, you aren't breaking any laws, putting any user data as risk, or being sued by InstaToonz. Sounds like a great option! But actually, you ARE putting user data at risk in a way. By not disclosing the bug, you leave the door open for a bad actor to independently discover the bug sometime in the future and compromise private user data. After all, if you could find the bug, couldn't someone else too?

***Part E:** Discuss whether the **ACM Code of Ethics and Professional Conduct** offers any relevant guidance.*

Section 2.7 of the ACM Code of Ethics says you should foster public understanding of computing and technology and specifically mentions that this includes sharing "vulnerabilities" with the public. So, according to the ACM, you have an obligation to make the security bug known to the public, so long as you can do it in a way that doesn't put user data at risk (that is, notify InstaToonz privately beforehand to give them time to patch it).

Part F:** **Describe and justify your recommended action, as well as your answers to any other questions you presented in part A.

My recommendation depends on who you (the bug finder) are. If you are financially and socially secure enough to stand up to InstaToonz's aggression, including the possibility of a lawsuit, then you should follow the industry standard and report the bug privately to InstaToonz. After giving them ample time to patch the vulnerability, you should share the bug publicly. This way, other programmers will be able to avoid making the same security mistake in the future. Also, it is important for InstaToonz users to know that their trust in the security of their private messages should not be absolute.

On the other hand, if you are not in a position to stand up to InstaToonz's aggression without suffering an undue personal burden, then you should simply keep the bug a secret, in my opinion. I do not believe you are ethically obligated to sacrifice significant amounts of your own money and time for the sake of InstaToonz's security. At the end of the day, the privacy of users' direct messages is InstaToonz's responsibility, not yours.

As to the question I posed in part A about how companies should handle security bugs, I obviously think InstaToonz is not handling this in an ethical way. But what is the ethical way to handle these situations, from the company's perspective? If you help a company improve its security by privately informing them of a vulnerability, you've done a service for the company and its users. So maybe the company should actually pay you! This is called a bug bounty, and several big tech companies do exactly this. But how much should the bounty be? How much does it take to incentivize people to report the bug instead of exploiting it? I'm not sure exactly how to answer these questions.