InstaToonz Bug Report

In this report we will be discussing the ethical implications of disclosing a bug that allows an attacker to read any private message sent by a user that has posted publicly before. This bug endangers the privacy of millions of users. The moral quandary comes from the fact that disclosing this bug threatens our own safety and wellbeing. InstaToonz has historically been aggressive towards a previous security researcher, and has publicly stated that they consider them to be stealing trade secrets. The main question is, do we disclose the bug to them? And if so, do we do it publicly so users know? Or, do we do so privately so malicious actors won't learn about it? And finally, what do we do if they decide against fixing it? We are currently assuming that the bug does not include encryption or copy-protection, but will discuss the changes in our scenario that the inclusion of these things would cause at the end of this report.

First it is necessary to assess the rights of each stakeholder in this scenario. InstaToonz, as the owner of the app, has a right to know about any possible data breaches and a right to protect their trade secrets and manage their systems. They technically have a right to distribute buggy software, but according to many US state laws, they don't have a right to hide data breaches from users[1]. Briefly, consider how App distributors have a right to know if the apps they provide are dangerous to users' privacy and a right to pull those apps from their services.

The users of InstaToonz have a right to privacy and confidentiality as well as a right to know what and when data has been breached. This also means that if we (the bug finder) personally saw any of their messages, the users have a right to know what we saw. Additionally, the users have a right to leave InstaToonz if they deem it insecure, but they may not have a right to wipe their data and messages, depending on the terms of service. Finally, consider the rights of the bug finder. In America, we have the right to free speech which means we can do what we

[1] https://www.malwarebytes.com/data-breach/

would like with the information found. However, note that it may not apply here because we would be sharing private information as well as possibly trading secrets (which is not protected). It is legally gray whether or not we have a right to reverse engineer the app, most likely not, but depending on our original intentions; if this is encrypted and copyrighted, our actions may not break DMCA[2]. We do not have a right to test exploits, and therefore should not experiment with the bug.

These rights and the legality of our actions vary depending on the details from the original situation. For example, how did we discover the bug in the first place? If we were trying to reverse engineer the program for valid reasons or if we stumbled upon it accidentally, we may be legally okay. If we were purposefully searching for bugs, we may be in legal trouble, as InstaToonz hasn't given permission to be digging around in their system. It is also necessary to consider what the terms and conditions are for the application. Do the users own their data? They have a right to privacy, but is it possible they waived it by using InstaToonz? It is important that we consider which state InstaToonz is based in. That would determine the specific laws that lay out if InstaToonz is responsible for fixing and disclosing breaches to users. Also, when recognizing if the application costs money, we feel there is a larger obligation from InstaToonz to protect and disclose what happened.

Listing out the possible actions for the bug hunter will help to determine the pros and cons of each option. The first option would be to release the bug publicly so that anyone could see its existence (full disclosure). The positive effects this would have would be letting users know that their data is not being kept private, probably urging them to take action of their own against InstaToonz. It would also give InstaToonz incentive to fix the bug. However, if the users instead are sent into a frenzied panic, there might be more harm than good. This option also

[2] See section 103(f) of the DMCA

proposes issues for the bug reporter as they share information of the website that can be traced back to them and therefore held responsible. The most detrimental consequence of publicly sharing this bug would be that malicious users could use the bug to exploit other people's private messages before the bug is fixed. This results in further endangering people's privacy and it would be the bug reporter's fault. There may be legal action that could be taken against the bug reporter for revealing it publicly, especially if the reporter is not anonymous.

The second option would be to disclose the bug privately. This would give InstaToonz time to fix the bug without alerting malicious users that it exists. However, users would keep sending messages over a potentially compromised program until the bug is fixed, and there is no guarantee that InstaToonz will alert the users or if they will fix the bug. If this is the case, the bug reporter then may wish to disclose the bug publicly. Disclosing the bug privately may also cause legal trouble for the bug reporter, as InstaToonz has a history of suing security researchers. The bug reporter may wish to disclose the bug anonymously instead. This may make it impossible for InstaToonz to ask important questions about the bug, but there are ways to be anonymous that allow you to respond. Even so, InstaToonz may still do nothing at all.

A third option would be to do nothing at all and hope InstaToonz finds and fixes the bug on their own. This is the safest option for the bug reporter but the worst option for the users and InstaToonz, as the bug may be discovered by malicious actors and exploited anyway. If we want to stand by the ACM code of ethics, this option is by far the worst. It maximizes the harm done for potentially millions of users and ignores their rights to privacy and confidentiality. The other two options are a little more complicated. Revealing it publicly increases the risk of harm by malicious users who weren't aware of the bug, but allows users to stop sending messages on an insecure platform. If there is an easy way to delete private messages such that the bug won't

display them, then the users also have a chance to hide their past messages. This gives the users power, but also puts them more at risk. Disclosing it privately will conversely minimize the amount of harm done, but this relies on the assumption that malicious actors don't already have access to this bug. Also, the users have a right to know about the breach, and reporting it privately means that InstaToonz may not disclose this information.

Our recommendation follows the principle in the ACM to contribute to society and human well being. We suggest disclosing the bug privately to InstaToonz pseudo-anonymously as to both protect ourselves and reduce the amount of unnecessary harm done. In the disclosure, let them know that they need to address the bug before X amount of has elapsed and if they do not comply, then the bug will be shared publicly. Worst case, you will end up publicly leaking the information and probably be involved in a lawsuit, but you may use the email/message you originally sent to prove your intents were for the purpose of helping the server and not for malicious use.

If you are able to leak the information anonymously, you would be able to avoid legal action while alerting users to the bug. Finally, if you saw anyone's private messages, you should disclose to them that their messages were breached and which messages you saw. If considering now that the InstaToonz app *is* encrypted and copyrighted, it would be even more important to disclose information anonymously to protect yourself from legal consequences.

There is an important moral quandary we have been ignoring. Do we have a right to hide? If we did break the law, legally we should not disclose information anonymously and should face legal consequences. But morally, we disagree. Assuming that you haven't exploited this bug for personal gain and you are only trying to secure the platform for the users and the

company, then it is morally right to protect yourself while disclosing this information, by disclosing it anonymously.

What option is best depends on the moral compass of the bug reporter. Also note, the legal consequences are much more extreme when the data is encrypted / copy protected which will further affect their final course of action. If they believe they should face the consequences of their actions, and are financially able to, then they may wish to attach their name to the disclosure. Whether or not to disclose publicly from the start is a hard question, as it may protect some users but it may put those who haven't seen the news in more harm. This is an incredibly tricky situation that has a lot of potential for harm but if you take the time to analyze the situation and the effects of your actions, you should be able to responsibly disclose the bug. Even if it ruins you financially or gets you into long and frustrating legal battles, at least you will be able to rest easy at night knowing you did the right thing. Long story short, get a good lawyer.