Main Ethical Questions:

Following the discovery of a bug in the InstaToonz DM system, we must decide whether or not to report the bug, and what manner in which to report the bug should we decide to do so. The company's dubious record of litigation against previous security researchers is concerning, but does not absolve us of our ethical responsibility to consider the full implications of informing or not informing InstaToonz.

Stakeholders:

InstaToonz Users

InstaToonz users are the primary concern of the bug and face the most exposure should the bug go public without a fix. Although privacy laws vary from state to state and get complicated very quickly, they typically depend on a "reasonable expectation of privacy."[1] A private message is assumed to have such a reasonable expectation.

Music License Owners

The owners of the licenses to music are also of concern here. Potential bugs in InstaToonz could allow unauthorized access to unlicensed music. This largely depends on if the bug involves the encryption and copy-protection of the music that InstaToonz users are sharing in their private messages. If it does not involve the encryption of the music, the license owners are not particularly relevant. If it does, we need to consider potential lawsuits by license owners over the illegal distribution of their music. As a security researcher, we may be concerned about violating the Digital Millennium Copyright act. Fortunately, under Section 1201.g.4.A

It is not a violation [of Copyright] for a person to develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research

Assuming that our discovery of the bug came solely out of a concern for the public interest, and that we don't distribute the knowledge for our own personal gain, there is minimal concern of litigation from this avenue. It is worth considering that releasing knowledge of the bug directly to the public without first informing InstaToonz could be construed as an action beyond "good faith encryption research" because it might allow other users to exploit the bug.

---

[1] https://www.thompsoncoburn.com/insights/blogs/internet-law-twists-turns/post/2016-07-12/do-you-have-privacy-rights-on-social-media-

InstaToonz

InstaToonz is a large stakeholder in the scenario. They may be responsible for the bug and face legal exposure if users' private information is exposed. They also have the rights to their app and its contained technologies, including the private messaging system. As with past litigation, they may choose to bring legal action against researchers who find bugs. Presumably, the above section of the Millennium Copyright Act would protect these researchers but they may still incur the financial burden of the lawyers required to defend against such a lawsuit.

The Security Researcher (Us)

As discussed above, there are potential risks to revealing this information. However, we should also consider our liability if we do not reveal the bug and it is later discovered by malicious actors. This would likely require retaining proper legal counsel with expertise in this area to provide a better understanding of our risk.

Potential Courses of Action:

No Disclosure:

Given the previous litigation against other bug reporters, we could choose not to report the bug. Depending on how easy this bug was to find, it could be some time before someone else finds it, or InstaToonz may be the first to find and fix it. However, there is also a substantial risk that a nefarious actor will find it (or may have already) and will illegally access other people's private conversations. Especially if InstaToonz is widely used, this could result in incredibly damaging and widespread leaks. Although probably not as bad as something like leaked credit cards or social security numbers, the end result would still be quite bad. Given the potential exposure, it is inadvisable to go with this course of action. Additionally, if it was later discovered that we were aware of this bug and chose not to disclose it, we could potentially be vulnerable to litigation from affected parties.

Full Disclosure

Another option that does not require interacting with InstaToonz would be to disclose the bug directly to the public. Although this would immediately make the affected users aware of the vulnerability, it would also reveal to would-be attackers the existence of this bug. Even if we did not directly disclose how to accomplish the exploit, the knowledge that it exists would likely be enough for attackers to find it. Additionally, InstaToonz may still sue or otherwise hassle us for revealing the bug. In the previous instance of a lawsuit by InstaToonz, it was dropped as public opinion turned against them. However, if we make no effort to resolve the issue by working with InstaToonz, the public may not view us as favorably. Additionally, as mentioned above, releasing the bug to the public without first informing InstaToonz may anger the license holders, prompting further litigation.

Coordinated Vulnerability Disclosure

Finally, we can try to report the bug to InstaToonz privately. The obvious drawbacks can be seen in what happened the last time someone reported a bug to them. InstaToonz may use lawsuits, harassment, or other intimidation tactics to discourage more security researchers from testing their application in the future. Given that this would be the second time, public backlash would likely come swiftly. Under coordinated vulnerability disclosure, we can also attempt to negotiate a date where we will release the bug to the public. This would allow InstaToonz time to fix the bug while still eventually informing the public that their data may have been compromised..

Ethical Considerations

The ACM Code of Ethics and Professional Conduct gives us a framework for considering the ethics of our plan of action. Section 1.3 states

Honesty is an essential component of trustworthiness. A computing professional should be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties. Making deliberately false or misleading claims, fabricating or falsifying data, offering or accepting bribes, and other dishonest conduct are violations of the Code.

The second sentence is particularly applicable, noting our responsibility to disclose the relevant information to all appropriate parties. In this case, the appropriate parties are likely InstaToonz and InstaToonz users.

Another potentially relevant part is Section 1.7

Computing professionals are often entrusted with confidential information such as trade secrets, client data, nonpublic business strategies, financial information, research data, pre-publication scholarly articles, and patent applications. Computing professionals should protect confidentiality except in cases where it is evidence of the violation of law, of organizational regulations, or of the Code. In these cases, the nature or contents of that information should not be disclosed except to appropriate authorities. A computing professional should consider thoughtfully whether such disclosures are consistent with the Code.

The bug likely puts InstaToonz out of compliance with general data privacy regulations. In this case, we have an obligation to at least report the bug.

Recommended plan of action

Given the ethical considerations and legal considerations, we are obligated to report the bug. Non-disclosure is too fraught with the danger of malicious actors gaining access to private information without anyone knowing. We must also decide whether to report the bug to InstaToonz or directly to the public. In both cases, we may fear the actions taken by InstaToonz against us, but giving InstaToonz some amount of time to fix the bug may improve public opinion of our actions. Given InstaToonz past record, our best course of action is to first inform them, but state that we will also release information about the exploit to the public in 1 week unless Instatoonz responds with a desire for more time and is cooperative rather than combative. Setting a stance such as this encourages InstaToonz to be cooperative while ensuring that the public will also be told about the potential for leaks.

It would also be helpful to know more about the uses of InstaToonz and its architecture. If the app is only ever used for sharing Music, the potential damage of this exploit may not be very large. If, conversely, the app is connected with a suite of other Insta apps, perhaps where some users conduct most of their daily communications, there could be a larger danger. Further, if the app is commonly used by government employees or other persons with sensitive knowledge, it may be important to promptly inform government agencies about the existence of this exploit.