Owen Barnett and Nick Pandelakis

CS 231

14 May 2021

In this situation, the relevant stakeholders are InstaToonz, myself, and the users of InstaToonz. InstaToonz has a right to encrypt their messages and source code, without people maliciously trying to violate their software. I should have the right to be protected from legal and financial harm for work that I have done to help people in good faith. I also have the right to not self-incriminate. Users have the right to privacy in that unintended or malicious people can not read their messages, or look at their message history. The main ethical question is: how can I protect the privacy of InstaToonz users without harming the integrity of InstaToonz software and putting myself in legal and/or financial risk.

There are a lot of specific details that might affect how I want to proceed. Perhaps the most important one is how I came across the exploit in question. Did it involve encryption or copy protection? Was I actively attempting to circumvent protective measures on InstaToonz or did I inadvertently stumble across this bug in some other non-malicious way? In the previous InstaToonz case, the FBI decided not to further investigate the bug-reporter in North Carolina. If I was trying to break into InstaToonz without their consent, however, the FBI might not be so lenient.

Regardless of the specifics of this scenario, however, InstaToonz has made it abundantly clear that it does not matter whether or not I violated section 1201 of the DMCA; they will still come after me for “attempted thievery of trade secrets.” My ability then to follow the ACM code of conduct is hampered by InstaToonz refusal to do the same. Section 2.9 of this code implores InstaToonz to integrate vulnerability reporting, but because InstaToonz has actively rejected this

code, it makes it extremely difficult for me to also abide by that code and be honest and protect InstaToonz's confidentiality. The code works best when all parties agree to abide by it.

For this reason, reporting the bug to InstaToonz without somehow masking my identity is out of the question. My options then are to report it to InstaToonz anonymously, disclose the bug to the public, or disclose it to law enforcement.

Reporting the bug to InstaToonz anonymously is not perfect. By protecting my identity, it will be very difficult for InstaToonz to contact me if, for some reason, they decide to change their stance on vulnerability reporting and do not want to sue me for attempted thievery of trade secrets. It also does very little to compel the company to fix the exploit. They may decide that if I am not going to release the bug to other people or exploit it myself, then the situation is as good as solved. Unfortunately, this outcome fails to protect the users' right to keep their private messages private. This course of action does, however, protect InstaToonz's rights to know about flaws in their system and to not have trade secrets disclosed to the public.

Another course of action could be to anonymously disclose everything I know to the public. In this scenario, I will still protect myself from InstaToonz's wrath and InstaToonz would be forced to fix their software or risk losing users, protecting users from further harm. Yet, by disclosing this vulnerability, bad actors will suddenly have access to an exploit they may never have found themselves. If InstaToonz can't fix the bug before hackers can exploit it, then I will have failed to protect current users' private messages.

Finally, I could anonymously disclose the exploit to law enforcement. This route would serve my interest by allowing me to disclose the bug without putting myself in InstaToonz's legal crosshairs. It may do nothing for the rights of InstaToonz and its users, however, since it is not clear what law enforcement would be able to do about it. InstaToonz is not committing a crime

by not patching an exploit they do not know about. If whatever law enforcement agency I choose to report the exploit has no obligation themselves to report this bug, then I will have failed to achieve anything by giving it to them.

The best course of action then seems to be to anonymously disclose the bug to InstaToonz and then the public at a later date. This would mostly protect InstaToonz's rights since I would not be disclosing a current flaw in their system to the public, giving them time to patch it. It would also compel InstaToonz to fix the bug before I release it to the public, protecting current users. The tricky part about this course of action is that it is unclear how long InstaToonz should have to fix the bug. It is not fair for me to unilaterally decide how long this bug should take to fix because I am not necessarily familiar with how InstaToonz implements their software. Because they refuse to allow for discussion, however, InstaToonz has forfeited their ability to have a say in how long a bug will take to fix. How I should proceed then might depend on how knowledgeable I am about computer security. In the case that I know a great deal about the subject, I may be able to effectively gauge the severity of the exploit and determine how long it should take to fix. If I know little about computer security, then it may be best to default to an established responsible disclosure framework, such as Google's 90 day disclosure deadline.

Ultimately, InstaToonz's failure to abide by the ACM code of conduct presents me with an impossible scenario. Their refusal to work with me, regardless of whether or not I may have violated the DMCA, prevents me from publicly revealing this exploit. Since it is not possible to publicly come forward with the bug, the only way to protect all the relevant stakeholders is to disclose it anonymously and take shortcuts in the normal bug reporting process. This course of

action does not perfectly protect the rights of everyone involved, but balances each party's rights as best as possible in the bug reporting climate InstaToonz has created.