

Miguel Alvarez, Martin Bernard, Fabricio Rua-Sanchez

As we think about this tricky scenario, there are a few ethical questions that we have to ask ourselves. For example, should we report the bug to InstaToonz? What would we accomplish by reporting this bug? What are the consequences of reporting this bug? What are the consequences of not reporting this bug? As security researchers do we have a responsibility to report these kinds of bugs? If there was encryption and copy-protection present when probing for this bug, this could also pose the question of, are we violating Section 1201 of the Digital Millennium Copyright Act?

Each party in this scenario: InstaToonz, the customers, the security researchers, and other similar companies have different rights and responsibilities. InstaToonz has the responsibility to protect their customers from infringements of privacy and data breaches but they also have the right to protect their trade secrets. The customers have a right to their privacy as well as a right to be informed of any potential breaches of security threats pertaining to their information. The security researchers have a responsibility to report bugs or vulnerabilities that can have a negative impact on a group of people, for example, the customers. Other similar companies have the responsibility to hold similar companies to a certain standard in order to protect the information of a group of people. If there was encryption present in this then InstaToonz has the right to how we found the bug considering we probably didn't ask an authority to gain access to the work to do "ethical hacking".

It would be helpful to know if InstaToonz is aware of the bug or not. It would also be helpful to know if InstaToonz maintains their original stance on security research.

We have a few ways to approach this problem: we can privately inform InstaToonz about the bug, we can publicly disclose the bug, we can take no action. If we privately inform

InstaToonz we could face the same consequences as the previous security researchers. This would mean the possibility of a lawsuit and FBI involvement. Even if we disclose the bug privately to InstaToonz there is no guarantee that they will resolve the issue. This would also give their customers a false sense of security since they would not be aware of the bug. If we publicly disclose the bug then the customers will be aware of the security threat but this would also mean that attackers could potentially use the bug to cause harm. However, the act of publicly disclosing the bug would force InstaToonz to take immediate action to resolve the issue, along with potentially gaining the support from the customer. If we were to take no action, this would not affect us in any way since we would not be putting ourselves in any sort of possibly legal trouble. This would also result in customers' information possibly being leaked if the bug were to be exploited and it would also probably not result in the fixing of the bug.

ACM code of ethics offers us a lot of guidance on the actions that we should take. The first code to offer us guidance is code 1.2 because of the harm that can occur with the bug not being resolved. We should take actions to avoid these harms. The next helpful guidance comes from code 1.6 because this involves privacy of customers and it tells us that we should respect it. Code 2.2 also offers helpful guidance, we as members of ACM have a responsibility to help maintain the high standards in computing. This means that we need to hold InstaToonz accountable for maintaining their systems to the high standards of ACM. Code 2.9 also gives us guidance on the standard of the security of computing systems. It states that "computing professionals should also take steps to ensure parties affected by data breaches are notified in a timely and clear manner," so we have a responsibility to inform the customers and the company. Finally, code 3.2 gives us guidelines on encouraging InstaToonz to act responsibly.

Given this situation, the response we would take is privately disclosing the bug to InstaToonz giving them a deadline to fix the bug. If InstaToonz doesn't not resolve the issue in time we would publicly disclose the information. This form of disclosure will allow us to attempt to work with InstaToonz to resolve the issue before risking the consequence of making the bug public knowledge. If InstaToonz were to refuse to resolve the issue then publicly disclosing the bug will allow us to garner support from the public to expedite the process of resolving the bug. We understand that by privately disclosing this information we risk the possibility of legal trouble with InstaToonz, however, we believe that the privacy and security of the customers is more important than the hassle of a potential suit. We also understand that if a suit is taken against us then we can use the leverage of public opinion to limit the legal action taken against us. We need to hold InstaToonz accountable to ensure that all other companies like them are kept in check.