CS: 338 - ETHICAL ANALYSIS OF A SECURITY-RELATED SCENARIO

Oliver Clay

SCENARIO #1: RESPONSIBLE REPORTING OF SECURITY VULNERABILITIES

A. The main questions related to "What Should You Do?"

The "you" in this scenario has the option of removing large, possibly widespread harm in return for potential personal hurt. The company will likely try to sue them if they report the bug. The last person who reported a bug did not ultimately face charges, but they were thoroughly hassled by InstaToonz. Even just getting hassled is tough enough. It can be a time consuming and expensive problem to navigate legal charges from a corporation. Given that the corporation released their statement that "security researchers" are criminals in their eyes, it is well known that the company does not want people digging around in their software, and this could be used against you in court. Yet, the ACM code of ethics cites that computing professionals should avoid harm and respect privacy, which you would be doing, in the utilitarian sense, even if your own personal wellbeing and privacy are put at stake. There is also some argument to be made about doing nothing at all. Assuming the bug hasn't already been found out by someone (if the attacker could use it undetected), a way of guaranteeing that nobody gets hurt is to simply do nothing at all. The bug will hopefully stay hidden until someone at the company patches it, and you wouldn't have to deal with the legality of everything. Lastly, we should address Section 1201 of the Digital Millennium Copyright Act, and whether or not it is violated in this scenario. If the bug involves the encryption and copy-protection of the music on InstaToonz, it could spell far harsher legal reprimandation, but you would only be violating section 1201 if you are circumventing some "technological measure that effectively controls access to a work." Largely, I don't think the bug involves music. The bug is involved with the personal messages of individuals on the platform, and the personal messages are not technological measures which control access to the music, but I would suggest speaking to a lawyer before reporting the bug, just to be sure. It is possible that the music which is "shared between users," as the scenario suggests, could be linked to the direct messages, and hence also compromised.

B. For each stakeholder, identify the stakeholder's relevant rights:

The company InstaToonz has the right to do their own business as they please; they have the right to their own privacy and to the integrity of their trade secrets. Whether or not you are accessing trade secrets by reporting the bug is for the court to decide. The company also has the responsibility to protect their client's right to privacy. By not adopting programs such as bug bounties, it could be argued that they are not acting with their client's best interests in mind, yet at the same time, the company is within its rights to rely on in-house employees for this bug spotting job, if they so desire. You have your own right to privacy, yet it seems that in investigating this bug you are violating the company's privacy, as they have previously stated they are totally against the kind of investigation you've done. Hence, if you act on reporting this, you would be violating one entity's right to privacy to potentially save the rights of another, albeit larger, group.

C. Missing Information:

Can individuals exploit the bug without the company knowing it? If they can, I would be more likely to report the bug because it's possible that individuals are already exploiting it.

What process did you do to find this bug? Is this a bug you found by using the software as intended, or have you been digging around in the code to find it. This could be useful in your own culpability, and in knowing how likely it is that someone else will notice the bug anytime soon.

How long were the legal proceedings for the previous bug reporter. Knowing how long or costly the process was will be a good tell at seeing how likely InstaToonz will be to fold if you also report a bug.

How applicable are some exemptions of Section 1201 of the Digital Millennium Copyright Act. The individual can be exempt from violation if such act is necessary to conduct for encryption research. This bug reporting isn't exactly encryption research, but if it involves a vulnerability within an encrypted system, I could see the definition being a bit more fluid than we would originally believe. Additionally, such exemptions are only available if the individual has gotten authorization before the violation of the policy. InstaToonz seems to be explicitly stating that they are not giving authorization, so I believe that you would be culpable, even if we are reading the heart of the law.

D. Possible actions and their consequences:

The first and most obvious possible action is to simply report the bug anyway. In this case, you would see a lot of legal pressure from InstaToonz, but you could be reasonably assured that they would have someone patch the bug in the near future, and that the details of the bug wouldn't be leaked before they could patch it. Another, albeit possibly less responsible thing to do would be to attempt to report the bug anonymously. I'm not sure if there is a great way to go about this, but it does seem to be the most beneficial thing to do, if everything happens to work out for each side. Reporting the bug anonymously would disqualify you from any of the potential good press you'd get for reporting the bug and possibly causing another cause célèbre, but it would save you the legal hassle. If you're reporting anonymously, it's possible that posting the bug to the InstaToonz site would put you at further risk, if they could somehow find a trail on you. A terrible thing to do would be to post the bug anonymously on a tech related form somewhere and just say "someone do something about this," but this could possibly cause the leaking of private information if other third parties exploit the bug before someone else reports it. Additionally, by not going straight to the company, you seem more suspect to criminal activity, leaking exploits behind their back. Lastly, you could simply do nothing at all. This is a very neutral path, nobody really gets hurt from it at the moment, but leaving the door open to future harm seems unethical also.

E. Guidance from the ACM Code of Ethics and Professional Conduct?

The ACM Code of Ethics and Professional Conduct has a few enlightening things about it. Overall, the code seems to be very utilitarian, preaching much about the good of all human well-being and changing the world for the better. If we are following the code to the letter. I'd say the best course of action is to report the bug in a trustworthy manner, giving details about the vulnerability directly to the company. This is the surest way to protect the privacy of the most people. Yet, the ACM Code also cites that one should strive to prevent harm, and I believe that preventing harm to yourself would be one way of interpreting this protocol. It could be argued, then, that in order to do lasting and safe work within computing, one's own work should be sustainable. I'm not sure if there is actually a right answer here, as the ACM Code is, as they say, "not an algorithm to solve ethical questions," but the but should ultimately get reported, hopefully in a manner that leaves "you" unharmed.

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

Ultimately, my recommended action is to go ahead and report the bug, despite the risks of retaliation from InstaToonz, or the risk of violating Section 1201 of the Digital Millennium Copyright Act. The ethical thing to do here is to act to protect the privacy of the large, vulnerable group of millions of users. I think that, depending on how deep you had to dig to find this bud, the company InstaToonz could make a strong argument that you are meddling in their company's private business, which they have explicitly said is against their policy. Yet, such policy is ultimately against the good of the individual, as it is putting their users at risk by attempting to silence you. I would say that the main way forward is to report the bug and probably cause another cause célèbre. The company will likely put pressure on you again, and you may have to pay fines, or even jail time if you are violating section 1201, yet there will likely be people fighting on your side in the tech industry throughout the process, as taking a stand like you would be doing here is the only real way to make positive change. Thus, report the bug, maybe get jail, or even a slap on the wrist, but you could ultimately pressure the company's policy to change, or even get a bit of notoriety which could land you a new job. It does not seem ethical to ignore the issue, or to throw the problem to others who may not have as good intentions as you do.