Skyler Kessenich and Grace de Benedetti
5/14/21
Computer Security
Jeff Ondich

Ethics Report

In this situation, we are faced with the problem of whether or not to report this bug to InstaToons. If we do decide to report it, we also must decide who to report it to. Should we report the bug privately to the company? Should we expose it publicly so that the company is under pressure to address it? What steps should be taken in delivering this information to InstaToons? Additionally, to protect ourselves, should we get our own legal counsel before proceeding with reporting the bug due to knowledge of the precedent?

We also must take into account the relevant stakeholders in our predicament. First, we need to think about the rights of the customers. They have a right to the privacy of their conversations and information, and this bug puts both of those rights in jeopardy. For example, an attacker could quickly get private information about customers and use it for malicious purposes to exploit them. If this happens, InstaToons would probably be liable. The next group that has rights is InstaToons itself. InstaToons has a right to its own data, a right to security against hacking, and a right to their trade secrets. If a hacker gets inside their system, all of these rights will be violated. Finally, we have rights as the person who found the bug. We have the right to an attorney and other legal rights if we are to be sued. We also have a right to share this information that we have found if we have found it legally.

A few additional pieces of information would aid us in our decision-making process of whether or not to report the bug and how. First off, we would want to know where we are located. Since InstaToons must have legal rights in certain areas where they are located, laws differ across states, and the previous legal battle occurred in North Carolina, gaining more information about our location could shift our decision because the local laws could be different depending on where we are. Additionally, how did we find this bug? Was it through legal avenues? Did we cross a line and hack into InstaToons illegally, meanwhile obtaining the information we should not have access to? Why did the FBI decide not to pursue the matter further? Does my situation resemble this previous example? Would the FBI again side with the security researcher if we were to be sued? Also, we may want to know how many users are on the app. If there are more users, there is probably more private information to be exploited, and thus, the consequences of an attack are much higher.

Now with just the information at hand, we can do three things. First, we could report the bug privately. If we do this, we allow the security/software engineers at InstaToons to possibly fix the bug quietly, as not to allow any attackers to know the bug exists. However, if InstaToons acts as it did in the previous case, we may get sued. Moreover, by not letting the public know of the bug, we give them a false sense of security that their data was protected. In addition, by taking this plan of action, we are adhering to many of the ACM Codes of Ethics. Specifically, we are avoiding harm, and we could argue we are contributing to society. To avoid the guilt of not telling the users about this bug, we could publicly report this information. Here, we would alert the users of this breach and choose whether or not to continue using InstaToons. However, unless InstaToons fixes the bug quickly, hackers know of the bug and could potentially hack the system. Also, we could still get sued. In fact, if this situation puts us in violation of encryption and copy-protection there is a strong case against us being liable so by reporting the bug either publicly or privately, we are even more open to lawsuit. In this situation, we are still in line with the code of ethics as we empower people and, in this case, probably be more trustworthy. Finally, we could choose not to report the bug at all. In this situation, we will not be sued, but we are not practicing good ethics. We are knowingly allowing harm to occur to people.

The ACM Code of Ethics does provide a helpful framework on how we should act in this scenario. One particular quote does help in our decision-making process. The Code of Ethics shares, “A computing professional has an additional obligation to report any signs of system risks that might result in harm. If leaders do not act to curtail or mitigate such risks, it may be necessary to "blow the whistle" to reduce potential harm.”

We recommend reporting the bug. According to the ACM code of ethics and our underlying morals, if we have found such a security threat, we must report it for it to be fixed. Regardless of the potential hassle, we might go through if InstaToons decides to sue, reporting the bug and protecting InstaToons users is the right thing to do. Sensitive information is at risk of being exposed, and the rights of the customers are at risk. Furthermore, we believe we should publicly report the bug. Since InstaToons does not have a positive track record surrounding reports of security concerns, we think reporting the bug publicly will pressure the company. Users of InstaToons will hear about the bug and likely complain or expect the company to protect their private information. Thus, we would expect a public report of the bug is likely to lead to better outcomes regarding a security fix by the company.