Emma Roskopf

Jeff Ondich

Computer Security

23 May 2022

Scenario #1: Responsible Reporting of Security Vulnerabilities

The main ethical dilemma that I am facing here is that I want to report this bug to protect the data and messages of all of the InstaToonz users, but if I reveal that I was poking around for this bug I could get sued for stealing trade secrets. InstaToonz is clearly unreceptive to people who find bugs and report them, which basically reduces my choices to a) telling them privately about the bug so they can try to fix it, run the risk of being sued b) tell the public about the bug, put people's messages at risk until InstaToonz fixes the issues, still risk being sued c) don't tell anyone about the bug, feel bad about about when someone exploits it d) try to submit some anonymous report or complaint so they can't sue me, who knows how effective that will be. Depending on how rich I am, there is also a choice a) subsection i, which would be to talk to a lawyer first and figure out the best way to report to InstaToonz and not get sued. Or subsection ii, try to sue them first under some tort law negligence case because they didn't catch this bug and put their clients' privacy in jeopardy. But I'm assuming this is me, like current broke college student me, so choice a) subsection i and ii aren't really options.

An interesting aside, I was looking up the legal protections for people who do bug hunts for companies that offer bug hunts. Even when companies do offer bug hunts, it's still legally murky because safe harbor language isn't always clear or standardized. So people still run the risk of being punished when reporting bugs to companies, especially small ones that aren't under as much scrutiny to make their bug hunts safe for bug hunters. But either way, in this scenario, legal bug hunting channels aren't an option since InstaToonz won't implement it.

For the people involved in this scenario, I think disclosing the information in some way is the best option. First off, as an ethical computer scientist I believe in doing the best I can and minimizing harm. If I let this bug exist and don't try to get it fixed, I know there is something harmful and not doing anything about it. Stakeholders are all of the people who use InstaToonz. They likely would not want to send messages if they knew that all private messages could just be extracted. Also InstaToonz is falsely promising them that private messages are private, and since I know otherwise I should try to help. For the consumers, having the issues fixed ASAP and being told that there was a security flaw would be the best option. InstaToonz's clients would then know that the issue is fixed, but it might have caused damage and if their data was leaked they can seek compensation from InstaToonz. InstaToonz is another stakeholder here, and they don't want people to be looking at their code. I've already broken that rule, so I would think their next most pressing interest in this case is that they would want to know privately about security issues to fix it without further damage happening. Publicizing their security issue in option b) would not do that, and likely would result in more losses to consumers until InstaToonz fixes their mistake. So we can effectively count out that option because it damages both categories of stakeholders unnecessarily. Plus I still get sued, so that's a lose-lose-lose.

I am fairly certain my best option here is still to just contact InstaToonz privately and prepare myself to get sued (win-win-lose). Things I would want to know more about would be the laws InstaToonz would try to sue me under, how the DMCA would impact my case, and how riled up I could get the tech world on my behalf (hopefully very, so InstaToonz will drop the case). I would probably try to build a strong case for myself as an encryption researcher so it would be harder to sue me under the DMCA section 1201. Because I'm taking a class about security, I would argue I'm "...engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology."[1] I'm for sure engaged in a legitimate course, I can make a case that I'm trained, and if I immediately report to the company privately to try to get everything fixed I have a pretty good case for classifying myself as legitimately doing it to improve the state of encryption and thus I'm permitted to circumvent encryptions and copyright. If I didn't have to mess with copyright then I don't have to worry about DMCA, and just normal suing for trade secrets. I would say I'm not in a great situation here, but the best option by far is reporting the issue privately and putting together a strong case in preparation of being sued.

[1] https://www.law.cornell.edu/uscode/text/17/1201