Thea Traw

Ethical analysis of a security-related scenario (#1)

The central ethical dilemma of this scenario is, essentially, to disclose or not to disclose? And if so, how? For the former, you must address the balancing act of protecting yourself versus protecting others. The threat of InstaToonz suing you for responsibly disclosing the bug is certainly non-zero (and given their past actions, high) which would potentially mean significant legal and financial consequences for you. But not disclosing the bug would mean that you are endangering the privacy of countless others through your non-action. (Or, at least, the guilt would feel very heavy if you didn't disclose and then someone less upstanding than you found the bug and acted on it.) The method of disclosure also matters, if you choose to go that route. You could anonymously report it, use a third party to do so, tell InstaToonz directly about the bug, or just go public. Which is the best option for you? For InstaToonz? For the users? And is that "best" choice the most ethical one?

Other auxiliary questions include various details about context. What were you doing to find this bug, and with what intentions? Were you trying to snoop on a specific person's messages, but then realized you stumbled into a much larger problem? Did you think you could pin the confession of misdeed to some crooked politician? Were you trying to enhance your personal experience with InstaToonz by changing a feature? Were you trying to bypass a technical protection measure because you were curious about what was being encrypted? Any of these pieces of motive could potentially change just how tricky it would be to defend yourself in court, should you be sued. A person who initially had gray intentions would perhaps have to summon more moral courage to responsibly disclose the bug than someone who just stumbled into it. But either way, you really have the ethical imperative to do so.

Another question to consider is whether you have reached out to the people whose private messages you saw (when you found the bug)? Is it better to tell them and potentially embarrass them or to leave them in the dark and let the matter resolve itself after you report the bug? And also, what happens if InstaToonz doesn't change anything, even after you disclose it to them? (They try to sweep it under the rug.) Do you go public anyway, even if that could mean that bad hackers capitalize on the knowledge before InstaToonz is now forced to fix it?

There are three main stakeholders in this scenario: you, InstaToonz, and the users of InstaToonz. You have the right to use the product you paid for (assuming you have a subscription to InstaToonz and are not pirating it), and sometimes using a service might result in the discovery of something wrong with it. InstaToonz has the right to protect their intellectual property, such as source code and content. The users have the right to know if their private information that is promised to be private is not actually secure. However, if there was some sort of contract agreed to in the making of an account (that has some clause about not being responsible for data leaks) and the users agreed to it–then the users technically gave away their right to that information. Everybody has the right to a lawyer and can sue another party.

It would also be helpful to know the following information. How did you find the bug, and under what circumstances? Was it located in the front-end code that you found after thorough inspection and fiddling? Did you receive back-end source code from other hackers? Or did it just happen when you were using the UI? That is to say, was it gross negligence of InstaToon to have released a version with this bug out into the world, or did it take some truly crafty thinking on your end to discover? Also, did you have to maneuver through any technical protection measures to find it (bypassing encryption, undoing obfuscation, etc)? Because that would cause the DMCA to kick in, which would potentially influence your course of action. Also, does InstaToonz make users agree to a click-through contract that forbids reverse engineering, viewing code, etc?

There are a lot of possible actions that you might take and their likely consequences. (Some of which are far more reasonable than others.)

- ➢ You could choose not to disclose the bug, and keep it private. It's not your problem that InstaToonz messed up, and you don't want to deal with the hassle of getting sued. You just hope that nobody else finds the bug before the InstaToonz people eventually do.
    - ○ Likely, someone else will find the bug, and they probably won't be as public-spirited as you are. This means that you had the opportunity to protect the privacy of countless users, and you squandered it in order to save yourself some trouble. It's not the worst thing you could do, certainly, but also not really that great either.
- ➢ You could submit an anonymous report of the bug if InstaToonz supported that ability (which they might do instead of the bug bounty, because then they don't have to pay anyone), and then hope that InstaToonz gets its act together and fixes it.
    - ○ Likely, this would be a perfectly satisfactory way to report the bug (unless you want some share of the credit and would rather not be an anonymous source). Once InstaToonz knows about the bug, they really do have to fix it, or you and every user could sue them for non-action on their knowledge of a known security issue. This anonymous report thus should compel InstaToonz to make the change and also alert the users to the vulnerability.
- ➢ If you happened to bypass a technical protection measure while finding this bug, then you would be found in violation of the DMCA. (For instance, maybe you undid encryption, or looked beneath intentionally obfuscated code, or tricked the software into doing either of these things for you.) So you might be protected by an exemption to the DMCA for good-faith security research. And then with that protection, you then report the bug to InstaToonz. They really shouldn't be able to do much to you, as the Library of Congress has stated that "good-faith" security research is excluded from DMCA.

    - This would be a very slow, cumbersome process. (And potentially in that time, some bad hacker could also find the bug and exploit it, before you even get the chance to disclose it.) So this would be a reasonable choice for you to make, and it would fulfill your ethical obligation to attempt to protect the privacy of the users as well as afford yourself some protection. But it is not the most practical choice and may very well be just too inefficient to do any good.
- You could report the bug to a third-party reporting group like CERT. And then let them take care of it.
    - Likely, as long as you choose a trustworthy group to hand the bug over to, then this is a good solution. You will be protected because InstaToonz would be hard-pressed to take on an established and reputable third-party, and you would not be the direct target. The bug would also go public in some set amount of time, which would force InstaToonz to make the change and not bury their heads in the sand because they are embarrassed.
- You could directly and responsibly disclose the bug to InstaToonz, hold your ground, and potentially get sued and lambasted by InstaToonz and their fleet of lawyers that they send after you.
    - Now, there are a couple of ways this could go. If you did not violate the DMCA at all, and you never signed any contract (or if it was a contract of adhesion and you *had* to sign it to get the product, but you didn't read it) that forbid the steps you took to find the bug, then you most certainly will be able to get your case thrown out, eventually. InstaToonz would still try to make a case against you, saying that you are committing computer fraud and doing something wrong, even if all you did was click some buttons or stumble upon a bug in the UI. But you would certainly have the facts on your side. But if you did violate the DMCA, and didn't apply for an exemption, that could make your case trickier to get dismissed, but it probably still would be with any reasonable judge. So really, it would just be a huge hassle for you, and a money drain. It also might make you a hero or a martyr to the ethical hacking community, though, so that could be fun.
- You could post the bug on some public platform and see who gets to it first, the InstaToonz people or the hackers.
    - You would be incredibly careless with the privacy of the users if you went this route. This is basically inviting the hackers to exploit the bug as soon as they can, and they probably would beat the InstaToonz people to it. (Especially if you posted after the work day ended.) This is only a good choice if you want to cause chaos and don't care at all about violated privacy.
- You might think that InstaToonz is too powerful and needs to be taught a lesson. You want to force them to implement a bug bounty. Then you might get an advocacy group on your side (like EFF) and raise a stink about the security vulnerabilities they are exposing all their clientele to. If you embarrass the company enough, maybe they'll change.

    - This could work to enact change, but it would not protect you from a lawsuit. You also are involving more people in the bug, which probably increases the risk that someone does something less than ethical with it.
- You could also throw your own ethics out the window, and make a profit by selling the bug on the dark web. Of course, then you certainly wouldn’t be looking to responsibly disclose (unless you want some sort of alibi or something). So you wouldn’t be in the quandary at all with this choice. You could also commit to a life of crime on your own by exploiting the bug yourself and gathering as much private information as you want on whoever you want. But again, that would rather preclude your urge to responsibly disclose, and you would be facing more severe and reasonable consequences should you be caught.

In regards to the ACM Code of Ethics and Professional Conduct, there are a few statements especially that apply on the ethical end of your decision. However, it does not offer any practical guidance on how to handle the legal or financial stress that you may be facing should you choose the ethical choice. I suppose that ethics here should come before you try to avoid hassle for yourself. The mandate to avoid harm (1.2) states that a computing professional should “report any signs of system risks that might result in harm.” That directly applies here. Also, even though you found a bug and did not write the code yourself, the statement to “design and implement systems that are robustly and usably secure” (2.9) also offers advice in that “parties affected by data breaches [should be] notified in a timely and clear manner.” Now at the point of your bug discovery, the breach has not yet occurred, but it is important to be timely. Dragging your heels or spending forever deliberating over what to do only introduces more risk to the privacy of the users, given that someone else could find the bug at any moment.

The best choice to make is, if possible, to use a third-party reporting system. You then have protection from InstaToonz as an individual, and you also fulfill your ethical obligation to protect the privacy of others when you have the ability to. (And if InstaToonz doesn’t fix the bug after it is reported, then you can sue them!) If that is not possible, however, the next best option is still to disclose the bug. You really can’t ethically just walk away from the issue once you know about it. (The occupational hazard of poking around in the code, I suppose.) You probably would have to either anonymously report it, or take some other method that expects a prompt response (directly reporting it, going public with an advocacy group). The lengthy process to get a DMCA exemption might be too long to be able to achieve the goal of protecting user privacy. You also really should let people know that you saw their private messages (if you know them), and otherwise just scrub them from your brain. It’s just for the best to let people know if you found out something that they thought was private. But in total, if you find a bug, you really are ethically obligated to inform InstaToonz as well as the users.