Doug Pham

Scenario #1:

A.

Some questions that I would ask right away is obviously what should I do but more specifically - “Should I report this bug publicly so that all users would be able to know that their private messages can be seen by attackers or report this bug privately to help protect InstaToonz and any stakeholders involved but still bring it to the attention of the company”. Another interesting question I would ask is if I should make some sort of public statement to the InstaToonz users or something more formal and responsible directed only to InstaToonz. I would also ask what exactly are the legal implications in this case, knowing if this bug involves encryption or copy-protection or not, could change how I would disclose this information.

B.

The InstaToonz users have their rights to confidentiality in their private messages as well as data security. InstaToonz themselves have the right to their own intellectual property and whatever trade secrets they hold.

C.

Some information that is missing in this scenario that would be helpful in making better choices would be knowing more details about how InstaToonz actually resolved the previous bug (if at all). They do seem to lack input from the public, since they denied requests to establish a bug bounty program, so if they did not end up fixing the previous bug, I would lean towards addressing the users rather than the company to let them know and maybe stay away from using the application. If they did end up fixing it then I

would consider making a more formal approach directed towards the company. Another piece of missing information that would be helpful is knowing if the bug involves encryption or copy-protection. If it were to be an encryption or copy-protection bug then I would know if the disclosure would violate certain laws in the DMCA and I would have to change how I proceed with my responsible disclosure. If it did not involve encryption or copy-protection, then I would be less concerned about violating DMCA laws. It would also be helpful to know the details of the last private bug report. If it was poorly written and very unprofessional, that would maybe help InstaToonz in their reasoning for trying to sue the reporter.

D.

I would say there are two routes of action. I can privately disclose the information to InstaToonz which may fix the bug and thus protect the user's privacy, but then I assume the risk that they sue me or use some sort of legal threat against me. Or I can publicly disclose the information which could force InstaToonz to respond (though it may be negative) but puts me at risk of violating some law.

E.

Looking at the ACM Code of Ethics, I think Section 1.2 brings up valid points: "Examples of harm include unjustified physical or mental injury, unjustified destruction or disclosure of information, and unjustified damage to property, reputation, and the environment." Note that this section prefaces each of these with unjust, which I think is the key word. When looking at the bug I think it is important to note the extent to which it can affect either party. Obviously in this case where private information of hundreds of millions of users have the ability to be exposed is unjust to the users. But perhaps in another scenario of less severity, attacking the company and bashing on them can

negatively affect all parties involved with the company. Employees, stakeholders, and families could be hurt unjustifiably with unnecessary public disclosure. I think this also ties in with section 1.5 which is respecting the work that goes into new inventions. A lot of work goes into developing intellectual property and in most cases it is not the intention of the workers to aim to hurt the public but sometimes mistakes do happen and to thrash a company and its employees is unfair. So when disclosing this information either publicly or privately, it is important to do so professionally.

F.

I would say the recommended action is to privately disclose the bug to InstaToonz. I say this because it aligns with the responsible disclosure as it won't hurt InstaToonz negatively as much as publicly disclosing it as users would likely have an negative response and thus end up hurting the company and any stakeholders. But it will still bring this bug to the attention of those at InstaToonz and showcase that there is a large problem that needs to be fixed. Also following the ACM Code of Ethics, it also minimizes the harm to every party which it emphasizes a lot. I would seek professional legal help to ensure that guidelines are being followed and no laws are being violated. But if the private disclosure is not well received and follows a similar path to the last incident, I think taking the public disclosure would be a better route.