Kevin Clelland

A) The main ethical question here is weighing the privacy of millions of users against the insistence of the company that your actions constitute attempted thievery of trade secrets, and possibly also violate their rights under the DMCA (depending on whether the bug involves encryption and/or copy-protection), and obviously it begs the question, “Should you report the bug?”. I think that’s the fundamental question, but there are also a couple more questions here worth thinking about, such as “Does the company have the right to intimidate security researchers this way? (and should we let them?)” and also “Don’t consumers have the right to know about potential risks of the product?” (this is why we have all those disclaimers in commercials after all).

B) I, as well as all of the consumers, should have a right to privacy in all of our private messages if the company promises us that their platform keeps our information private. However, it also seems at least somewhat likely that there might be a clause in a terms and service agreement somewhere (that probably no one read) that either waives this right or shields them from liability so long as they are not found to be at fault for the release of our private information.

On the company's end, they I would argue, have significantly more rights, particularly if the DMCA is relevant. The software belongs to them, and the problem with code is that fully examining it inherently means one could in principle completely copy it, so bug hunting, if sufficiently invasive, could constitute thievery of trade secrets.

Furthermore, if there’s copy-protection code involved, and I have found a way around it, it is illegal 1) to do that, and 2) to share that information with anyone, and the DMCA offers them a very solid ground to sue me, if I do that and then present them with evidence of me having done that.

C) I would like to know how easy it is to stumble upon this bug. If it’s easy to stumble upon, then I think the ambiguity is removed from the situation, and the bug has to be reported. If it’s a fairly subtle thing, I still think it’s important to report (I don’t think there’s ever an amount of obscurity that makes it decidedly the better option to not report), but the ethics I think become less one sided in that case.

Also, I’d like more information on how practical it would be to submit something anonymously to people in the company who have the ability to fix the bug (or people who would pass it along).

Finally, in the case that there is encryption and/or copy-protection I would like to know specifics about how I found this bug, and what exactly I appear to be circumventing to know whether or not I would be in violation of the DMCA.

D) There are, broadly speaking, two actions: report and don't report.

Let's look at don't report first. If you don't report then you won't get sued by the company, and assume essentially no risk whatsoever, so this is the good option on a purely individual level. However, that's not the level on which you should consider this, because your silence could result in the privacy breaches of hundreds of millions of users, which is extremely bad, and I would argue is negligence in your duty as a good programmer. So the don't report choice has no assumption of risk, but potentially does harm to hundreds of millions of users.

If you do choose to report however, it seems likely given the scenario that you'll have a lawsuit on your hands, and no matter who you are, losing that lawsuit would be very bad for you. For your efforts though, as long as you can report the bug privately, it will probably protect hundreds of millions of users from a potential privacy breach. Do note though, that it's preventing an event that could potentially have a very high or very low probability of actually occurring (although if someone stumbled upon it it's probably not too low). So for this choice you assume a large risk to prevent the possibility of something extremely bad happening.

I'd like to mention one other thing though, which is that thievery of trade secrets is a federal crime, so you'd have to be unanimously convicted by a federal jury of 12. If InstaToonz has hundreds of millions of users, the odds are pretty good that a couple of them are sitting on your jury. So if you really play up the "I protected your data" angle in court, you might come out ok, and the other good news is that that probably doesn't count as jury tampering.

Finally, I'd like to mention a sort of third option you have, which is to try and report something anonymously, so InstaToonz, Inc. can find no one to sue. This may or not be practical, and an anonymous complaint could definitely result in no change at all, but this might be a good first step that could potentially protect you from a lawsuit while also preventing the privacy breach.

E) The ACM Code of Ethics and Professional Conduct says both to Avoid harm and Respect privacy, which I think falls pretty clearly on the side of reporting the bug privately. So I think that's what should be done in this scenario.

F) In my opinion, this constitutes far too great a risk to not bring up to the company, so I would report the bug. Probably what I would do is first attempt to send this tip anonymously to the IT team at InstaToonz, Inc. and hope that the issue will be solved without me ever being identified. If that failed though, I think I still would report the bug. Consumers have a right to the privacy that they are at least strongly led to believe they have. Furthermore, I think in the interest of security in the long run, it is important not to let companies intimidate the work of security research just because it might damage their reputation. Sure, it's hard maybe even impossible to beat the hackers, but if we don't try, that's something even worse. So I would do what I had to to protect the privacy of those hundreds of millions of users, and be sure that federal jury knows it.