Ethics

Scenario #1:

Author: Lily Li
Conferred with: Jeff Ondich

Sources:
https://www.eff.org/zh-hans/deeplinks/2021/11/honoring-aaron-swartz-aaron-swartz-day-2021
https://www.schneier.com/blog/archives/2022/05/the-justice-department-will-no-longer-charge-security-researchers-with-criminal-hacking.html

Note:
Green font analyzes the option with Digital Millennium Copyright Act violation
Purple font analyzes the option without violation

A. Main Ethical Questions

In both cases, I think the ethical question is whether to ensure your personal safety/career or to risk your life for the benefit of other people, and expose the bug in InstaToonz (publicly or privately) —- What should you do? Should you care more about the entirety of your life, the life of the people closer to you, or the benefits of other people you don't even know? And also, how should you do it? Does ethicalness have levels? Is it okay for you to violate some rights of the company (which may be slightly unethical) for the greater ethics, the benefits of millions of users?

Taking one step backwards, if you were an ethical hacker of good faith, the moment you decided to hack, *you are already facing an ethical dilemma* —- whether to stay far away from the 'gray zone', or to risk potential punishment/trouble for your investigation so that some vulnerabilities may be discovered. Therefore, I think if you are an ethical hacker, you must already be a brave person, and to some extent have already made a decision on the possible choices that you may encounter in the future.

However, let's say you decided to do something. What happens if the sharpest tool you thought you had had no effect at all? For instance, you wanted to force InstaToonz to change their code through public pressure. But what if the public/users didn't care (anything can happen)? What if something you thought was a big deal gained almost no reaction from the public? And what if InstaToonz doesn't care about public opinion at all, or didn't need to?

Maybe people got mad at InstaToonz and made it infamous. Eventually, InstaToonz had to shut down because it had no users anymore. However, InstaToonz is owned by a mega-conglomerate Mega-Insta, and they have hundreds of APPs like InstaToonz under their wing. All they had to do was shut down InstaToonz and create another music APP and market it, NewInsta. They could even move all the former employees of InstaToonz to NewInsta, and EVERYTHING ELSE STAYS THE SAME. And they still have hundreds of millions of dollars to prosecute you. You may have a family, people who depend on you to survive. You may have friends, people who will get threatened/tortured for things you've done. These are all things you need to consider.

So the question might become: Are you willing to risk ***your all*** for the ***possibility*** that something good may happen? But also, could you live with yourself if you know this harmful bug and decided not to do ***anything*** about it?

B. Stakeholders and Relevant Rights

The ethical hacker (You):

- The right to utilize your knowledge without breaking the law (hacking ethically with permission or with authorization).
- The right to hack secretly, but you will need to be responsible for the consequences.
- The right to express your opinions, positive or negative.
- The right to expose sensitive information, but you will be responsible for the consequences.

Company (InstaToonz):

- The right to decide what they do with their product, to fixs/not fix bugs and add/not add features.
- The right to process the information they own (i.e. user information that belongs to the company under the *user terms/privacy policy* agreed upon)
- The right to not disclose vulnerabilities I*nstaToonz* for a certain period of time, under the *Coordinated Vulnerability Disclosure* vulnerability disclosure model.
- Copyright/patent/trademarks of I*nstaToonz*

Artist (Musicians who put their music on InstaToonz):

- The right to decide what to do with their music, whether to remove it from a platform or not (unless there was a contract involved which they agreed to give the music out)

- The right to not disclose any personal information they have not agreed to disclose (i.e. personal messages)
- The right to have their registered music protected under Copyright and other laws
- The right to know that if there may be a vulnerability in the application that will violate their rights
- The rights to express their opinions, positive or negative.

Regular user (Regular users who use InstaToonz):

- The right to not disclose personal information unless they agreed. (i.e. in user terms)
- The right to use/not use the APP
- The right to know if their rights may be violated
- The rights to express their opinions, positive or negative of the APP on any platform

Country (Under which the law operates):

- The right to require its citizens to follow the Copyright regulations
- The right to punish citizens for not following the law.

C. Missing Info I'd Like to Know

- Is InstaToonz a 100-people startup or is it a conglomerate like LVMH
- Is 'you' single or has a bunch of family responsibilities
- Which country does 'you' reside in
- How good is 'you' as a hacker, is 'you' the type of hacker that can wipe out all of their traces from the internet and actually achieve anonymity when exposing sensitive information?
- How easy is the bug to access? Is it an extremely elusive and hard to exploit bug, or would it easily be found and make the headlines tomorrow?
- What is the financial status of 'you'? Does 'you' rely on a 9-5 job to survive?
- What is the *privacy policy* of InstaToonz? Does InstaToonz automatically own all of those messages (so technically even if they leak the messages, they are not breaking the law)
- Does InstaToonz have any major competitors that at least seemed to be more concerned about ethics?

D. Possible Actions & Consequences

If there is a potential violation of copyright law, any bug revelation may result in jail time, probably destroying your career (if you still want to work somewhere). Given the history of InstaToonz, if you report this bug to them privately, they'd probably be the first to sue you with their best lawyers for violation of Copyright and happily send you away. Unfortunately, no matter to whom you expose this bug, you will always risk getting into trouble because you would've indeed violated a law.

If you didn't violate Copyright, you might not get into jail. The Justice Department had said that they will no longer charge security researchers with criminal hacking:

“The policy for the first time directs that good-faith security research should not be charged. Good faith security research means accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability”

Although the idea of ‘good faith’ seems ambiguous and may be argued upon but at least that means you may not be charged. However, depending on the loss you caused InstaToonz, many terrible things could still happen….. You could lose your career, or even more….You may also resort to organizations like ACLU(American Civil Liberties Union) or EFF(Electronic Frontier Foundation) for protection or support. However, there are still people who they weren't able to save. Aaron Swartz, for instance, suicided at the age of 26 in the face of a long sentence because he broke the Computer Fraud and Abuse Act (CFAA) by hacking into Jstor. If you are in the US, your actions have probably already violated CFAA, and any exposure of your identity would put you at risk.

So, in both cases, I believe that the best thing to do is keep your identity secret
You can choose to publish this bug anonymously, use a tool like Tor and hop between multiple servers across the globe. Unfortunately, as Jeff mentioned, almost anyone could be found with enough money invested. Maybe InstaToonz is a mega-corporation, and they wouldn't hesitate to spend a few million dollars on finding you.

And in both cases, I don’t think it’s a good idea to report this bug to InstaToonz privately. Your intention must be that you want something to be done. Given their attitude, I don’t think anything will be done if you report to them in private. So you may have the following options (just some examples, not exhaustive)

1: *(Difficulty: B)* You could secretly contact a journalist and let them publish this story. Journalists have regulations under which they could protect their source. But for your safety, it's best that you don't let the journalist know who you are. Consequences may include:

- The journalist's story is not well received and nothing really happens
- The journalist's story is not well received, nothing really happens but InstaToonz decides they will dig you out and retaliate (but it'd be harder given the journalist could protect you under law and all that).
- The story created a storm, and the public hated InstaToonz. No one uses the app anymore, and all the musicians sue the company and the company is bankrupt, *yay!*
- The story created a storm, and the public hated InstaToonz. No one uses the app anymore, and all the musicians sue the company. However, the company is part of a huge conglomerate and they fixed this issue quickly. The conglomerate just launched a new app and continued whatever they did. Public opinion may be important but sometimes it's not enough to be deterministic. An example suggested by Jeff is the company Equifax, who leaked the credit scores and personal information of 147 million users in 2017 due to not updating their software in time, and they are still in business today doing what they do! No one likes them but they still have the privilege to do the business they do. More info from : https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

2: *(Difficulty: C)* You could consult a lawyer for advice. Lawyers are under stronger mandatory laws to protect your information (even criminals hire lawyers) so maybe they have better advice but I could not predict.

3: *(Difficulty: C)* You could post on the forum anonymously, with tools like Tor.(Not recommended though given that it seems like with enough dedication, anyone behind the screen could be found) Consequences may include (similar to what was discussed above):

- Nothing happens and your forum wasn't even noticed
- The forum exploded and you were found and retaliated and got into jail, but InstaToonz ran out of business and many users were protected.
- The forum exploded and you were found, but didn't go into jail. Nevertheless your personal life was destroyed, but InstaToonz ran out of business.
- The forum exploded and your life was obliterated, but nothing serious happened to InstaToonz. This is a very probable scenario given capitalism, or that it was explicit in the *privacy policy* that the company owns all these direct messages,

and they have amazing lawyers. Through some legal meandering, InstaToonz walks out intact

4: *(Difficulty: A)* Leak this information to someone of greater power, a major competitor of InstaToonz or a famous artist who puts their music on there. They may have more resources, and power, to actually solve this problem by exterior pressure, given that InstaToonz doesn't seem like they are going to address it because of any interior reasons (Required discretion, need to really scrutinize whether this is a conscious company or not)

5: *(Difficulty: S)* Rally power to fight InstaToonz together. You contacted the bug-reporter in North Carolina and maybe discovered that there are other incidents in which InstaToonz acted like a jerk. You gathered all the victims of InstaToonz's actions and you contacted someone with political power to hopefully lobby against the company.

- It was a big success. Hit the national news and a bill went through and put an end to InstaToonz and all similar actions by tech companies.
- Nothing progressive happened, but your life is ruined (90%)

5: *(Difficulty: SS)* Compete with InstaToonz so it runs out of business. You've decided this company is no good and you will build a new App to out-compete it. Given that InstaToonz doesn't even approve bug bounty programs, you can tell that they lack respect for both their users and the technology itself —- how good could their APP be?

- It was a big success. You fully respect user privacy. Your APP is always up-to-date with the latest technology/protocols/vulnerabilities. Your APP is transparent to the maximum. As a result, users naturally choose to use your APP. InstaToonz becomes obsolete and everyone is using an APP that is safe. After you gain significant power in this industry, you expose the bug in InstaToonz. You are your own boss, no need to worry about your career anymore! And, you are on par with InstaToonz, you guys now have similar powers and you are not afraid of them anymore.
- Before you could do any of the abovementioned the bug was exploited and many people were hurt

6: *(Difficulty: SSSS)* You expose the bug to the public anonymously and ensure that InstaToonz will never be able to know that you did it. I don't know how you could guarantee that but good luck. In that case, nothing bad will happen to you and you can continue your life.

E. ACM Code of Ethics and Professional Conduct Guidance.

Following this general principle:

> 1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.

I feel like you are obliged to report/ expose the bug, even if maybe no positive results were received. Because *contribution* doesn't equate to *result.* Maybe your contribution wouldn't create a change, but it will definitely accumulate towards a positive change. And millions of people are using this APP, that is millions of potential victims.
However, as we read through this principle:

> 1.2 Avoid harm.

You have to admit that you will be potentially harmed. Even the police department ensures their personal safety first, before helping others. This is especially true if you are just a CS nerd who doesn't have significant social powers. Part of being an ethical hacker must also be to protect yourself from unethical harms. Especially as it says in the website too. "In either case, ensure that all harm is minimized"

I am especially inspired by this professional responsibility:

> 2.7 Foster public awareness and understanding of computing, related technologies, and their consequences.

Maybe this is the ultimate best way to do it. As also mentioned by Jeff, the laws are often written by people who have little understanding of computers, and if everyone could become more aware of these issues/dilemmas then maybe this will become less of a problem.

F. Recommended Action

In either case, consult a lawyer, follow their recommended practice to try your best to conceal your identity and expose this bug to the public, whether or not it's through contacting a journalist in a phone booth anonymously. Given the actions of InstaToonz, the potential harm is too great to bet on the slim possibility that they will

accept the private report and fix their bug. InstaToonz is used by millions of people, and most probably hacked by thousands of people too everyday. It is unlikely that a bug will remain not exploited for a long period of time (even APPs themselves won't last that long!)

There is a risk in doing anything, also in ethical hacking itself. So I think as long as you have tried your best to minimize the risks and are aware of the outcomes, you should follow your conscience.

Even though I painted a lot of dim possibilities in the first part, that doesn't mean nothing should be done. All changes are hard, and it's even harder for people who are participating in the changes. So it should be expected that the reality would be far from your expectations, and anything could happen and drag you down.

Also, dedicate yourself to the public education of ethical hacking. What is it? Why is it important? What can those companies do with your data? A lot of people are taken advantage of because of their lack of understanding in computers/softwares. Many people have no idea what it means when they click the 'agree' button on the *user terms* for their APPs. With more widespread knowledge, it will affect legislation someday, and someday, ethical hackers would hopefully not have to struggle in ethical dilemmas anymore.