Soren DeHaan and Carl Tankersley

A. Identify the main ethical question or questions faced by the main character ("you") in the scenario. This will certainly include "what should you do?", but there may be other interesting questions to consider.
    - What should you do?
    - What is the relative value of your own personal legal liability vs the security of the data of the company and its users?
    - What is the relative value of a company's desire not to have bugs reported vs the security of its users?
    - How to tell a company that it's being dumb?
B. For each stakeholder (or category of stakeholders) in the scenario, identify the stakeholder's relevant rights.
    - Oneself: right to autonomy, right to privacy, right to transparent communication, right to restrict access, right to confidentiality
    - The company: copyright, right to privacy, right to transparent communication, right to restrict access, right to confidentiality
    - The customers: right to autonomy, right to privacy, right to transparent communication, right to confidentiality
    - The artists: right to autonomy, copyright, right to privacy, right to transparent communication, right to restrict access, right to confidentiality
    - The record labels: copyright, right to privacy, right to transparent communication, right to restrict access, right to confidentiality
    - The company's shareholders: no rights for these leeches on society
C. List any information missing from the scenario that you would like to have to help you make better choices.

- Who is in charge of InstaToonz's anti-knowing-about-critical-security-flaws policy, and are they persuadable?
- Does InstaToonz seem appeased with their earlier bout of sabre-rattling, or are they likely to do it again? Related: was this an isolated incident, or has this happened on other occasions?

D. Describe your possible actions, and discuss the likely consequences of those actions.
    - Option negative one: exploit the bug yourself. Woo-yeah! Get that private information and become a criminal for no particular reason! Yeah!
    - Option zero: announce it to the world. This is very dumb: you will probably get arrested and/or sued, and it's likely someone would breach security before they can patch it, and it would also cause unnecessary financial instability. To reiterate, this is very dumb.
    - Option one: you could just tell them in private. However, you are probably gonna get sued and then everything is bad.
    - Option two: don't tell them. Then they're probably going to get a security breach, and a lot of private information will be made available, when we could have avoided the incident.
    - Option three: tell them anonymously (i.e. burner email). It is possible that they would ignore the information (or it gets filtered out as spam), though it's about as likely to happen as with the private report. They can't really sue, so this seems like a reasonable option, and it doesn't seem illegal?
E. Discuss whether the ACM Code of Ethics and Professional Conduct offers any relevant guidance.
    - Not really… it says not to do options negative one or zero, but that was kinda obvious already. It also recommends not doing option two, but again, that was clear.

- One point of confusion: since most people presumably already have a personal code of ethics, what role does a second one play? If the codes conflict, people will prioritize their personal one, and if they agree, they would've done it anyway. It also doesn't discourage malicious activity, because that is always done outside standard ethical frameworks regardless. The last role I can see is to bring up ideas that may have gone unnoticed, so is the ACM code of ethics just akin to a checklist of considerations?

F. Describe and justify your recommended action, as well as your answers to any other questions you presented in part A.
    - We recommend option three, at least at first. It does not detract from the company's copyrights, nor rights to privacy, confidentiality, or access restriction. It does not fulfill the right to transparent communication, but the transparency in a non-anonymous bug report is liable to restrict one's own rights to privacy and autonomy. With regards to the questions in part A, we elected to prioritize data security before company preference for willful ignorance, and aimed for a solution that would not put legal liability and data security in opposition.