\Ethical analysis of a security-related scenario - Devin Dennis

Scenario #2: your company's customers' personal data

1. 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.

The ethical dilemma is whether or not to oppose the CEO's proposal to keep from selling and storing user data, given that the company was founded on not storing users' data. I think that it's my responsibility to at least bring the founding ideas of protecting users' privacy to the CEO's proposal and see if that's still a possibility. Obviously, we don't want to deceive the users by now, all of a sudden tracking their location and storing it. I feel that if the CEO's really want to go about with this change to track data for up to a week, then the users must be clearly informed about how their data will be used. That way, users can decide if they want to continue to use the app, knowing their location data will be stored for a week. I think if the CEOs want to go about selling the user data anonymously, then this is something that I wouldn't stand by and advocate to keep their data internal. I think this is a great middle ground that allows for the CEO to still benefit from this new implementation of the app while still living up to the initial goals of the company.

2. For each stakeholder (or category of stakeholders) in the scenario, identify the stakeholder's relevant rights.

The users of Beerz have several fundamental rights at stake in this scenario. They have the right to informed consent regarding how their data is collected, used, and retained, which means they should understand and agree to any changes involving their personal location information. They possess a right to privacy and meaningful control over their personal location data, which is among the most sensitive types of information someone can share. Users also have the right to expect that their data will be used only for purposes they've explicitly agreed to.

The Beerz company and its shareholders also have legitimate rights that must be considered. They have the right to pursue this new change to allow new revenue streams that could ensure the company's sustainability and growth. The company has the right to modify its business practices as market conditions change, though such modifications come with the obligation to do so transparently and with appropriate disclosure to affected parties.

As someone working on the project, I have the right to work in an ethically sound environment that doesn't compromise my professional integrity, and I have the right to decline participation in practices I consider fundamentally unethical.

3. List any information missing from the scenario that you would like to have to help you make better choices.

- I would need to know the privacy laws for our users.

- The terms of service and privacy policy that our company promised about using their data
- Understand how, if possible, to protect the rights of our users by selling/keeping anonymous data and how it would it even benefit the company financially.

4. Describe your possible actions, and discuss the likely consequences of those actions.

I think I would need to set up some time to discuss the implications of selling the data with the CEO. We would need to go over the legal and principles of the company and how that would affect them financially, and the vision of the company. I could raise formal objections through proper channels by documenting concerns and presenting an analysis of privacy implications and legal risks, which would fulfill my professional responsibility but might be perceived as insubordinate.

5. Discuss whether the ACM Code of Ethics and Professional Conduct offers any relevant guidance.

The ACM Code of Ethics provides clear guidance for this situation. Principle 1.6 on respecting privacy states professionals should collect only the minimum necessary information and retain it only as long as needed. The CEO's proposal to mine archived logs and indefinitely retain data for monetization directly violates this, which is why it's important to go over the implications of selling the user data. Also, principle 1.2 requires avoiding harm, including to privacy, and retroactively commercializing data collected under different pretenses violates user expectations. This is important for making sure we are not selling data. Principle 2.5 obligates us to give comprehensive evaluations of systems and their impacts, meaning I must provide leadership with complete information about privacy implications, legal risks, and alternatives. Looking at the possible legal risk is vital to understanding the next steps. Principle 1.3 on honesty and trustworthiness means the company cannot simply abandon its stated commitment to discarding data without transparency to users. This is vital to make sure our users know what data is being collected and stored and what it's being used for.

6. Describe and justify your recommended action, as well as your answers to any other questions you presented in part A.

I recommend advocating to preserve the company's founding privacy principles while proposing a transparent compromise if necessary. My first step would be to meet privately with the CTO/CEO to align on approach, then present leadership with a comprehensive analysis of both the ethical problems and viable alternatives.

If the CEO insists on retaining location data for one week to enable the popularity features, I would argue this must be accompanied by complete transparency. We must update our privacy policy to clearly explain the new retention practices and notify all existing users of this change, giving them the choice to continue using the app or discontinue service. This

respects user autonomy and maintains the honest relationship we established with users who chose Beerz specifically for its privacy commitments.

However, I would draw a firm line at selling user data, even if anonymized. This crosses into surveillance capitalism territory that directly contradicts the founding vision. I think surveillance capitalism is ultimately harmful to society, just to squeeze as much capital out of our users. I feel that it’s not necessary, given that we have many other avenues to generate revenue.

The suggestion to mine archived logs from version 1.0 deserves explicit rejection. Those users shared location data, understanding it would be "immediately discarded." Retroactively commercializing that data is not just unethical but potentially illegal under CCPA (at least for California law), which requires data to be used only for disclosed purposes.

This approach acknowledges legitimate business pressures while maintaining core ethical principles. I'm seeking solutions rather than being obstructive, while establishing clear boundaries based on professional ethics. The ACM Code gives good guidelines to protect users, provide risk analysis to leadership, and maintain trustworthiness in systems I build. By proposing transparency for necessary data retention while firmly opposing commercialization, I'm providing an avenue that enables desired features while preserving user trust and protecting the company's reputation. I think user trust is more important than making as much money as possible in the short term. It takes years to build, and we wouldn’t want to break the relationship with our users. If leadership insists on data commercialization despite understanding the risks, I think that this company wouldn’t be for me.