Alex Falk

Ethical Analysis of a Security-Related Scenario (Scenario #2)

A. As made clear by the outline of the scenario, Beerz was built on the idea that user's location data is protected and eventually discarded. You were explicitly told that "We're not going to participate in surveillance capitalism." With the new developments (even, in a way, your own Beerz 2.0 ideas), this commitment to user privacy is thrown out the window. Now you must ask yourself a few questions about what to do.
    a. Do you talk to the CEO about this new development? You joined the company because of their commitment to user privacy. The possibility of sharing user data goes against this stance. Another interesting question could be raised here. Is the user data still being protected? Since the proposed system would anonymize the location data, users of the app would not be identifiable by this data. However, even if this is true, it could also be argued that selling someone else's personal data is unethical as is.
    b. Do you alter your plans for Beerz 2.0? Maybe you realize the best way to avoid this conflict is to change your plans, thus no longer requiring user location data to be stored for a long period of time. This might keep the location data sales off of the markets for at least a little longer. This question might be useless, though, in that the cat has already been let out of the bag. This CEO seems like they are here for the money and it's hard to get that tune out of their head.
B. Stakeholders and their rights
    a. Users: The users of Beerz have a right to privacy and a right to dictate how their information is used if it is used at all. It's objectively moral and ethical to acknowledge and respect these rights, regardless of whether or not it's protected by law.

b. The company: It's not made clear in the scenario what the laws are surrounding the use of users' data. If it can be used, I think the companies are allowed to slip this data usage clause into their TOS so that use of the app requires that users consent to having their data sold. If there are no laws protecting the users and their data then maybe since they collected the data themselves they are able to use it as they would like. In this case, it's moral to not sell their data but profitable and legal to sell their data.
c. Shareholders in the company: They want money. If it's legal and gets them money let's assume that they'll agree to it. They have the same rights as the company but they can claim less knowledge of the overall going ons in the company.

C. Missing info
   a. It would be helpful to know the state's/nation's laws regarding the use of user's data. Are there loopholes like anonymizing the data? Is consent required?
   b. I would like to know Beerz's outward message on data usage. In the interview it seemed like the company held a firm stance on not using user's data for purposes beyond that of the app. Is this a shared commitment? Is it shared internally (within the company)? Does this company make this explicit on their website? Do the users know about this commitment? If so, this makes the Beerz 2.0 controversy even harder to navigate.

D. Possible actions
   a. You could tell the CEO that you're not comfortable with the new changes and that you joined the company on the premise that they continue their commitment to not use user's data past the apps intended purposes. This would likely put you in the bad graces of the CEO as they see you as a barrier to money. It also might

not do anything. The CEO could tell you that their word is final and that they want you to go ahead with your previous plans.

b. You change the plans for Beerz 2.0 so that user data is no longer stored. The CEO might overrule this change and you'd be in their bad graces.

c. You do as the CEO suggests, implementing a feature that anonymizes user data and then puts it up for sale. You may find yourself in the bad graces of those that you work with, specifically the CTO who hired you. When the feature is released, depending on the local laws, the users might be made aware of this change. This could lead to less app usage and user backlash. The CEO could pass the blame off to you as you're the one who originally suggested that user location data be stored for a longer period of time.

E. Yes, it does. The Code says that individuals have a right to know what a company does with their data and a right to protection of their data. Therefore, if Beerz is to sell their users' data they are required to be forthright about it. Additionally, if they do end up selling the location data, they must also guarantee that the anonymized data is truly anonymous. If the location data is traceable then the company is at fault for possibly endangering their customers.

F. If the CEO already has moneybags in his eyes there is not really a choice. However, my recommendation would still be to scale back the Beerz 2.0 update. In doing so I would be keeping with my own moral code as well as staying true to the mission set out by the company during the interview. I do not want to author something that I believe could cause harm. I believe that the CEO only cares about the money and not the privacy and security of the users. This will undoubtedly lead to more creative differences in the future.