Hannah Scooler - Scenario 2

The main question in this scenario would be whether it is ethical to use data about user locations post hoc, that would have been logged when they believed that all of their data was protected and immediately discarded. This would be violating the trust that they placed in the company, since users did not give permission to store this data in the original application. Also, if the End User License Agreement included wording that mentioned that the location data would be immediately deleted and not used, then this also becomes a legal issue. Either way, it would be a betrayal of the users' trust to utilize data that they thought would be private. The issue is particularly exacerbated by the fact that the CEO seems to want to use this information to sell user location data, so the manipulation of user data is not even used for the user's individual gain. It is completely unethical to profit off of another person's data, particularly when that person did not provide explicit consent. There is also the ethical question of whether storing user data for a week is alright, since it is not strictly necessary. However, I think that since the features it would allow would be beneficial to users, and as long as users are properly informed of this change in policy, then it would be sufficiently ethical to proceed. Finally, another question is whether it is ethical to maintain the log, knowing that it provides the opportunity to use user location data that should have been immediately discarded. It would be one scenario if the company was unaware of this use of the log, but now that they are all aware of the implications, I think that the only ethical way to proceed would be to erase the log and have the data stored in a different way in the future. Again, I believe that it is extremely unethical to tell users that location data is discarded immediately but then to have this source that violates that premise. This is simply lying and violating a user's privacy and trust.

Some of the stakeholders include the company and the users. Foremost, the users have a right to privacy. This includes their location data, since this could be used to track an individual and potentially risk their safety. Also, the users have a right to know what is going on behind the scenes in this app that they are using. They should be sufficiently informed before any data is collected on what data is used, how it is stored, and what the company is using it for. If and only if the users provide informed consent to relinquish information, then companies can collect this data and use it for their own purposes. Especially if this data is going to be sold, the company has an obligation to inform users about this so that they are not being robbed of their information. However, if the user gives permission to the company to use their location information for whatever purposes the company outlines, then the company does have a right to make a profit. Since it requires money to help a company succeed, particularly a start-up, the

company has a right to find sources of income where it can. However, they should only be able to make a profit on information or goods that they actually own, which isn't the case with data unless the user gives that permission to the company to own and sell the data. Overall, the dilemma in this case is the battle between a user's right to privacy and a company's right to earn money, although I believe that the users' rights are far more important and inherent and should be prioritized well over the fiscal rights of a company.

I personally think that this scenario is pretty ethically clear, there is no ambiguity over which should be prioritized: my personal job, or potentially millions of users' privacy. However, I think that it would be even clearer if I knew for sure that Beerz had told users that their location would be deleted immediately. If Beerz had retained the right to store and use all location data in the user agreement at their discretion, then this would not be as big an issue, since the company would not be going back on their initial word. However, from the wording of the scenario, it seems as though this was not the case, and that users were informed that their information would be discarded and protected. I would also like to know the legal implications of selling customer data, although legality and ethicality are not always equal.

I have three options here: refusing to implement the features that would take prior data and presenting on why it would be wrong, whistle blowing, or going along with the plan regardless of concerns about user privacy. I think that the first option would be best, which would involve talking to the CEO and other shareholders about why utilizing prior user information or current user information without updating the license would be immoral. It appears very likely that I would have the backing of the CTO and perhaps other colleagues, so it is not necessarily a given to assume that this would happen at the risk of my job, especially at a beginning startup. At best, everyone will agree with me and commend my morality. If this does come at the expense of my job, then I should let users know about what might be happening with their data at Beerz, particularly if the company remains shady and unclear about their actions. Since whistleblowers tend to be protected from legal repercussions (not sure if this applies to company whistleblowers or just government ones), this might not even affect me negatively. There is also the option to simply ignore the ethical dilemma and proceed with the plan to utilize this data without the permission of users. The only real consequence of this would be the guilt that I would feel from profiting off of unknowing victims, but that's enough to make me not consider this option. Even if the company were punished for their use of location data without consent, since it was the decision of the CEO and the idea of the coworker, I would likely not be reprimanded just for implementing it. However, I still think that this would not be a viable or sustainable option for me.

In the ACM Code of Ethics and Professional Conduct, the first thing I noticed was that it mentions that “the public good is always the primary consideration”. In this scenario, that would mean that my own personal concerns of getting fired should not be given more importance than the violation of the rights of the public users. The Code then mentions that computers have an obligation to protect the right to autonomy, which would not be upheld if the company went through with this project. It states that “when the interests of multiple groups conflict, the needs of those less advantaged should be given increased attention and priority”. In this case, the conflict is between the interests of privacy and of profit. In this case, the less advantaged would be the users, who are getting their data used unknowingly, rather than the company that would be making money off of this. Thus, the Code states that the interest of privacy should be of greater concern, and so we should not be using the data without permission. While there would be no direct harm in using this data, there is no guarantee that there would not be an indirect or unintentional harm of the users, and there is no ethical compulsion to use their data in spite of this potential harm. Most relevantly, section 1.3 mentions honesty and trustworthiness. In this scenario, the company would need to be transparent about this change of data collection, and delete all the information in the logs, in order to be trusted by the public in the future. Finally, 1.6 mentions respecting privacy, which would not be done if the company sold information about a user’s location to other people/companies. Therefore, there is nothing in this Code of Ethics and Professional Conduct that would support selling user’s data and collecting data that they thought would be discarded, and in fact there is much to discourage it.

With all of this in mind, I think that it is pretty clear that my recommended action would be to mention the ethical implications of using and selling old data that users did not know was collected, and to refuse to build any software that would be betraying the privacy of users. This can be done respectfully to the CEO and coworker, but mentioning legal implications and the brand of the company could be a good way to convince them if they are unmindful of the ethical repercussions. I think that it is a good idea to go to the CTO first and see if they have any additional perspectives and/or would be willing to bring up this issue instead, given their higher priority in the company. From there, it is in the hands of the CEO to make sure that the company follows the ethical route, as laid out in the Code of Ethics and Professional Conduct