

Lane Maitland

I will be exploring the ethics related to scenario #2.

The main ethical problems faced by “you” in the scenario are the following:

- Do you feel like a more successful employee if your work produces new features or if your work prevents the storing/selling of user data?
- Do you feel comfortable utilizing user data that was collected before users were aware that their data was maintained?
- If profit is a concern, do you prefer raising the user subscription fee or selling user data?

There are multiple stakeholders in this scenario with different rights. One stakeholder is you, and you developed the idea for this project (the two new features of the app). Thus, you should receive credit for the idea and be able to largely control its implementation. Other opinions are valuable and should be thoughtfully considered, but your co-workers should not take your idea and run with it, leaving you out.

Another stakeholder is the software designers at the company. They should have access to legal/accurate data in order to build/test the features of the app. They should also be aware of how their work and final product will be used. They should not be tricked into creating features that are ultimately used in ways that they do not support. For example, if they are told that users must consent to their data being collected, the software designers may have no reservations about implementing data-collection processes. However, if they later realize that these processes are being used without user consent, they may feel that their skills have been taken advantage of, and they may feel guilty for assisting in unjust practices.

Another stakeholder is the managers at the company. Their job is to motivate the success, growth, and profit of the company, so they have a right to obtain profit from the work of the company. This profit should also benefit the other employees, but the managers should not be silenced for advocating for the profit generation.

A final stakeholder is the users of the app. They should know what data is being collected and when, and they should feel confident that their data is being stored securely and anonymously. No one should be able to “get all the old location data out of the API's archived web logs.” If the users are told that their data is maintained for only one week, this should be true.

To better understand the scenario, I would want responses to the following:

- How do you best serve users?
 - Do users care more about the app providing accurate recommendations or the app deleting their data after a set time period?
 - Do users prefer paying a higher subscription fee or consenting to the sale of their data?
- Who is benefitting from the storing of data?
 - Is the main purpose to effectively implement the features for the users or to generate profit for the company through its sale?
- Will users be informed that their data is being collected and stored and sold?

- Will users have the ability to decide whether their data can be used to generate the feature statistics?
- Who will be able to access the data?
- Who decides what happens with the data?
 - It seems that the CEO and CTO have differing opinions about this.

There are several possible decisions with a variety of consequences. If the app does not maintain the data for longer than one week, then building/testing the features may lead to inaccurate results. This would cause users to miss out on possibly helpful information/recommendations, and it would cause the company to fall behind others with a similar consumer base. With less demand for the app, the profit would decrease.

If the company utilizes previously collected data that is not supposed to be accessible, then building/testing the features could lead to more accurate results, but users would lose trust in the company, and the company could face legal consequences.

If the company increases the subscription fee to prevent the need to sell data, then some users may feel frustrated, which could cause the consumer base to shrink.

If the company sells data, then profit would increase, but the company could again face legal consequences.

If the company informs users that their location data is going to be maintained (not removed after one week), then users would feel that the company is honest. Some users may stop using the app, but others may join due to optimism about new features and comfort with the storage of location data.

The “ACM Code of Ethics and Professional Conduct” offers some relevant guidance. To avoid harm, the company should consider if selling data puts anyone at serious risk.

To be honest and trustworthy, the company should ensure that users should know how the app works and that software designers know the managers’ intentions for the use of their work.

To respect the work required to produce new ideas, the users and managers should know that new features pose a risk and will require new testing and security methods. The company should also provide credit to the creators of the ideas and the creators of the code that implements the ideas.

To respect privacy/confidentiality, the data should be stored securely and anonymously. Again, it should not be possible for someone to retrieve old location data from archives. The company should thoughtfully review which employees and outside entities have access to the data and how.

To design/implement systems that are robustly and usably secure, the company should consider how data will be collected such that it can be used as needed and permanently removed after.

To ensure that public good is the central concern and that special care is taken of systems that become integrated into the infrastructure of society, the company should create and present the app in a manner that encourages responsible drinking behaviors. While this guideline does not relate as strongly to security, it is still important. This app and its features appear to motivate users to attend breweries and drink beer, which have associated safety concerns. The app should not inspire users to try every brewery and beer in a single day, and it should never reward users for visiting breweries more often or drinking more beer than nearby users.

I think that our personal data is always being collected. While that can be worrisome, I do also think that it creates benefits. I would encourage the company to inform users that their data will be collected and to begin building/testing the features with this data. That way, the data used has been acquired with consent, and the features can be developed legally. While maintaining data may cause some users to leave the app, I think that many others would join, so I still foresee the demand and profit increasing. If this holds true, I would advise against raising the subscription fee. I would support the sale of the data only when users are informed and when strict measures are in place to ensure that no one unintended can access the data. I would also require the company to permanently delete all previous data, as it should not be accessible.

I think that the information and recommendations given by the features (made possible by the access to a large set of location data) could be very valuable to users of this app. I also anticipate that it could be useful to other apps and services, so selling the data to other companies could have positive outcomes for the users as well as the company. It could help restaurants and stores decide where to launch, as consumer preferences or demographics may differ by area.

To be explicit, I feel that the answers to the beginning questions are as follows:

- Do you feel like a more successful employee if your work produces new features or if your work prevents the storing/selling of user data? → produces new features
- Do you feel comfortable utilizing user data that was collected before users were aware that their data was maintained? → no
- If profit is a concern, do you prefer raising the user subscription fee or selling user data? → selling the data