Lily Haas

Ethical Analysis of a Security-Related Scenario

Scenario #2: Your Company's Consumers' Personal Data

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.

There are two main ethical questions posed in this scenario. The first is whether it is ethical to switch models from scrubbing user data instantly to anonymizing and selling that data. Originally, the company was committed to staying out of the realm of surveillance capitalism, deleting user location data as soon as the API returned the list of nearby breweries. This was likely part of the draw for many users and could result in customers not returning if this changes with the next update. The second question is whether the company should retrieve data that was not supposed to be stored to sell. This would be a blatant violation of the users' trust and depending on the terms of service and user agreements, could also be a violation of contract with the users.

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

There are several relevant stakeholders including the customers, the company, any stockholders, the platforms the service is distributed on, and whoever is buying the data. The stakeholder with the most rights in this scenario is the customer. When purchasing a subscription for this app, the customer had the understanding that their location data would not be stored or sold. Thus, they have the right to privacy with their location data. Selling data that had been stored without customer knowledge would be a clear breach of this right. The company also has some rights in this scenario including setting the terms of service for its app. If the company wishes, it may change the terms of service in a way that it could collect and store customer location data. If the company were to change its terms in this way, it could do so in a way that applies retroactively as that would infringe on the rights of the customer.

Moving on to the stakeholders not directly involved in the agreement between company and user, the stockholders of the company have a right to know decisions the company is making and have influence over them. This means the company should inform them if planning on making such a change. The platforms distributing the app (App Store, Play Store, etc.) set their own terms of service that the company must follow. If the company violates these, the platform can remove the app from distribution. The potential data purchaser does not have any rights in this scenario as no deal has been written.

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

Some missing information is the terms of service and user agreement between the company and its customers. For the sake of argument, I have assumed that it makes the promise the CTO advertised about not storing or selling user data. I also wonder why the API archives have the location stored. In my mind, this is already a breach of privacy whether the data gets pulled and sold or not. Why was this not written in a way that either redacts the location from the logs or purges it? If this were due to negligence, the data should be destroyed immediately and an apology to customers should be issued. If it was intentional, the company should investigate it and make sure there has not been a data leak before destroying the information and apologizing to customers.

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

There are a few possible actions including going with the original plan of continuing to scrub data just on a weekly basis instead of immediately, changing the terms of service to allow for the sale of anonymized location data, and selling the old data. The first option is the safest, there may be some users who dislike their data being stored for a week, but an opt-out feature would likely satisfy them. Changing the terms of service to allow for the storage and sale of anonymized location data would likely lose some more security-minded customers but most likely most of the userbase would continue their subscription. The last option could result in the destruction of the company's public image. If users learned that their supposedly deleted location data had been sold there would be public backlash. Additionally, the wording of the terms of service could result in legal action against the company by users.

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

Section 1.3 of the ACM Code of Ethics is incredibly relevant to this scenario stating, “Computing professionals should not misrepresent an organization's policies or procedures”. Stating that the company is committed to avoiding surveillance capitalism while selling data that was supposed to be deleted would be a clear misrepresentation of policy and procedure.

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

My recommendation would not vary much from the presentation given in the scenario, the only modifications I would make would be to make this optional. Any user can opt out of prompting to contribute their data, receiving data from other users, or both. Those who do not opt out will be given the option to check in at a brewery and rate their experience with “bad,” “neutral,” or “good.” This not only helps protect user data but also prevents the app from recommending breweries that customers do not like. Then for the comparisons with other popular breweries the app will only display pairs where both breweries were rated “neutral” or better. As a last feature, if a user chooses to opt out or unsubscribe at any time, their data will be immediately scrubbed. With this strategy, customers are always aware how much (if any) of their data is being stored and can have it removed at any time. These changes will not alter the company’s original promise not to sell data and still ensures data is scrubbed, just not immediately unless by customer request.