ETHICAL ANALYSIS OF A SECURITY-RELATED SCENARIO

By: Sydney Nguyen

Note: The following information and analysis will be extracted from scenario 2.

Main Ethical Problem:

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.

Do I allow my CEO and company to falsely advertise what is done with their data?
Does profit outweigh privacy?
Is there a way to privately store information and locations and not be tied to specific users?
Does morality outweigh income?
Do I whistleblow?
Do I continue to create the app features even though it goes against what the CTO wants?
Is there any possibility that the company can safely handle the users information where we are not abusing the infromation?
Can I implement these features where I make the information gained from the breweries nad not by users of the app rather just the traffic of the store?

Stakeholders Context:

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

Users: The app users and clients have the righ to their privacy. Also the right to know their data is being collected, used, and shared.

Beerz inc: The company has the right to commit to any changes and production of their services within the law. The right to work in the interest of capitalistic gains.

You: The knowledge and weight on you as, you created an app that unethical collects and uses clients data. Since you brought up this idea if and when things go awry you will be most likely used as a scapegoat. You also have the ability to leave the company whenever desired.

Breweries: The right to sponsor certain advertisement and having their brewery associated with this application.

Important Infromation:

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

What information so far have we given to our users on the data we collect?
Is there any way we are able to track solely the location of the data?
Does the CTO actually have an influence on decisions within the company?
Do the GET requests with data location ever get deleted?
How do we store the data?
What security measures do we have?
Can you easily get a new job for money sake or does the job market suck?
What harm will come if the data is sold?

Possible Resolutions:

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

You could simply ignore your moral ground and continue to produce the app that utilizes users data without their consent. It would most likely come with a pay raise and the continuation of your emplotment at Beerz. You would be able to work and gain the favor of your CEO but fall into bad graces with your CTO. Also should be notes that in the situation that the information is leaked about using the data without consent we will lose the trust of the customer and most likely use my job at Beerz.

We can go to our CEO (hopefully with the support of the CTO) and propose to only use the newly gathered data and have users opt in or out on data collection. This may come with the cost of not being as financially beneficial for the company, or there will be no change on the financial gain. We may have less users as people are afraid of having their data tracked.

Implement the app, but make the data anonymous and not infringe on the privacy of the users. This may be very hard and you may not be rewarded for besides the nice warm feeling in your stomach that you did something right. You will be in good graces with the CTO and okay graces with the CEO if the financial gain is the same.

You could attempt to form a coup type situation gaining the support of your coworkers and threaten a walk out if things are not changed in the company. There may not be enough of your coworkers that will support you. Also should note that you have already given your idea and the framework to the company so you can now be easily replaced unless the implementation is much harder than I think (which is very possible).

Quit, you lose your job probably are unemployed for a period of time and blacklisted to a degree because of your company and not complying with their wishes.

ACM Code of Ethics and Professional Conduct:

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

Section 1.1 - All people are stakeholders in computing

This obligation includes promoting fundamental human rights and protecting each individual's right to autonomy.An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy. When the interests of multiple groups conflict, the needs of those less advantaged should be given increased attention and priority.

We as programmers need to be aware of the possible danger we are putting others in as we create the app and mitigate the consequences of using our customers information.

Section 1.2 - Avoid Harm

In this document, "harm" means negative consequences, especially when those consequences are significant and unjust. Examples of harm include unjustified physical or mental injury, unjustified destruction or disclosure of information, and unjustified damage to property, reputation, and the environment. This list is not exhaustive.

We would be specifically going against this section as we have the potential dicolsue their, customer’s, information through collecting data and utilizing it in our application.

Section 1.3 - Be trustworthy and honest

Honesty is an essential component of trustworthiness. A computing professional should be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties. Making

> deliberately false or misleading claims, fabricating or falsifying data, offering or accepting bribes, and other dishonest conduct are violations of the Code.

We are breaking this section through lying by omission.

Section 1.6 - respect privacy

> Computing professionals should only use personal information for legitimate ends and without violating the rights of individuals and groups. This requires taking precautions to prevent re-identification of anonymized data or unauthorized data collection, ensuring the accuracy of data, understanding the provenance of the data, and protecting it from unauthorized access and accidental disclosure.

In no way have we given any interest into anonymizing our data we should take steps towards this to help have our app gain ethical infomration and use it in ethical ways.

Section 2.7 - Foster public awareness and understanding of computing, related technologies, and their consequences.

> Important issues include the impacts of computer systems, their limitations, their vulnerabilities, and the opportunities that they present. Additionally, a computing professional should respectfully address inaccurate or misleading information related to computing.

When we as a company refuse to tell the public we are collecting their data and the usage/possible consequences that come from our collection and usage of the data.

Section 3.1 - Ensure that the public good is the central concern during all professional computing work.

> The public good should always be an explicit consideration when evaluating tasks associated with research, requirements analysis, design, implementation, testing, validation, deployment, maintenance, retirement, and disposal.

We are not taking the public good into account when we are using their data without their consent.

Recommended Action:

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

I recommend to in the next opportunity speak to the CTO as well as propose anonymizing the data collected from our customers. Making it a point to the CEO with the support of hopefully the CTO that it is important to ethically collect and use data. Highlight the importance of trust and transparency between the company and customers. Another improvement we can make is adding proper security measures to the the database where we keep all our customers information. Protecting our customers information would also mean we should not sell out customers information without their consent and understand of what their data will be used for because of the ethical dilema. We need to be also constantly making sure to not keep old data and clean the database as to prevent overflow of information, as well as make our database less attractive to hack as it does not contain a lot of location data. Another important point is to solely collect the customers location at breweries not general location or other information from their device. To support our arguments we can use the ACM sections to show the ethical sections we will breaking and what our company is assumed to do. It should be assumed before you have this discussion you speak with coworkers and the CTO to get backup and show the CEO the actual importance of the issue at hand. If the CEO and company does not make the correct ethical changes you can always just leave the company, and whistleblow to the press.