Ruben Boero

ethics.txt

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.'**
    a. Is it worth the extra revenue to infringe on the privacy of the user a little more?
    b. If the user location data is stored in the API logs, then was it really ever discarded like the CTO said?
    c. How safe is anonymized location data? How is it anonymized? Is it really anonymous, or can it be reverse engineered so that it's no longer anonymous?
    d. If the code is buggy, is it safe to move on with storing private information?
    e. Who has access to the data before it is anonymized? Is there a way to make sure that if an employee peeks at the non-anonymized data they can be caught?
    f. Who will we sell the data to? Will there be a vetting process to attempt to verify that the person buying the information isn't intending to use it for nefarious purposes?
    g. Will I lose my job if I don't do what the CEO wants? Is it worth it to me to lose my job over this issue when there are clearly other people at the company who would happily implement the data tracking that the CEO wants?
    h. How much extra money would the company make? Is it worth exposing user information for not much extra revenue?
B. **For each stakeholder (or category of stakeholders) in the scenario, identify the stakeholder's relevant rights.**
    a. Users
        i. Right to know what data is being tracked, and how it is used.
        ii. Right to a useful product that works as advertised
    b. Employees
        i. Right to a non-hostile work environment. If I believe that implementing a certain feature is unethical, I should not be punished for it.
    c. Higher ups
        i. Right to have a say in the product that is being created
C. **List any information missing from the scenario that you would like to have to help you make better choices.**
    a. Can we ensure that the anonymized information is truly anonymous?
    b. Is the CEO knowledgeable in security like me? Have they considered the ethics of the situation as well? Do they fully understand what they're asking me to implement?

c. How much power does the CTO have? It seems like they don't like the idea of tracking user data. Can I ally with them and have a meaningful conversation with the CEO, or will we be brushed off?

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

a. Implement the data tracking feature to appease the CEO and make more money
   i. CEO is happy
   ii. Users are exposed to greater security risk
   iii. Company needs to spend much more energy making sure that the user's privacy is maintained

b. Do not implement the data tracking feature
   i. CEO is unhappy
   ii. User's privacy is upheld
   iii. I could get in trouble
   iv. Company goes under because they need the additional revenue from selling data

c. Find a pseudo middle ground. Perhaps allow the user to easily opt out of the data tracking feature.
   i. The compromise hopefully makes all the shareholders feel somewhat satisfied.
   ii. Extra money is made, but most likely less than if the user is forced to opt in to the tracking of private information

d. Talk to the CTO and discuss options before doing anything
   i. Hopefully I feel better about my decision and don't make any enemies at work

e. Talk to the CEO and discuss options before doing anything
   i. Hopefully I feel better about my decision and don't make any enemies at work
   ii. I could change the CEO's mind if they were not aware of the potential security risks

f. Talk to both the CEO and CTO to discuss options before doing anything
   i. Combination of d and e

g. Talk to a third party (significant other, sibling, trusted friend, etc.) before doing anything. (Consulting someone not within the tech bubble.)
   i. Hopefully I feel better about my decision now armed with a "non-techy" person's opinion/assessment of the situation

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

a. "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."

   i. The interests of the higher ups in the company conflict with the privacy of the user. We should prioritize the user because in the power dynamic of developer and user, the user is less advantaged.

b. "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."
   i. Regardless of the choice we make, we should let the user know exactly how their data is being used. I think this includes letting them know how their data is logged and how it's scrubbed.

c. "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. Computing professionals should establish transparent policies and procedures that allow individuals to understand what data is being collected and how it is being used, to give informed consent for automatic data collection, and to review, obtain, correct inaccuracies in, and delete their personal data."
   i. If I choose to implement the data tracking, the way that we anonymize the data is very important. (It should really be anonymous.) Additionally, we should allow the user to access and modify the data that we are storing about them.

d. "Personal information gathered for a specific purpose should not be used for other purposes without the person's consent."
   i. It should be clear to the user that their information will be sold, not just used within the app.

e. "3.1 Ensure that the public good is the central concern during all professional computing work."
   i. I don't think that making the most money possible is for the CEO is a public good

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

I recommend that the company not implement the data tracking feature. I also recommend that the company rethink how it stores API logs/how the user information is sent in the first place. The way the system is set up now, it doesn't seem like the data was actually being scrubbed.

The idea of storing user data to make more money in addition to a subscription fee seems scummy and greedy. Not only is it unnecessary, it also exposes the user to privacy concerns. (Who will have access to their information? Will it remain anonymous?) Additionally, there are multiple sections of the ACM Code of Ethics that refer to working for a common good, and I doubt that the type of companies that peddle in personal information are bettering the public good. Unless the extra revenue is being donated to charity, I don't see how it could be seen as bettering the public; and even if the money was donated, there's still the ethical issue of whether the money received is worth the risk that the user is put into. The code of ethics states that computing professionals should aim 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." In the context of this ethical debate, selling private data *increases* threats to safety, security, and privacy. As I mentioned in bullet E-a-i, I interpret the user as being the less advantaged group compared to the CEO/developer of the app; as such, I believe that the user information should not be stored for more than a week, nor should it be sold. The user loses in the scenario where their personal data is sold. They gain no added functionality from the app and they are at greater risk for their information to be stolen.

I would sleep better at night knowing that there is no possibility that I've ruined/complicated someone's life because their location data got out to some nefarious person. It's not impossible for the data to get out while it's in the system for a week, but I imagine the longer information is stored, the more likely it is to be leaked somehow.

As for answers from part A, I can't provide answers to any of these questions as they are open ended and/or no context is provided in the scope of the question.