Authors: Charlie Roslansky, Silas Rhyneer

Scenario #2

A. Main ethical question(s)
    a. Do you let your colleague and the CEO run with the idea of selling location data, or do you put a stop to it?
    b. Can you implement your features while still maintaining user privacy?
    c. Do you have to alert users if their data is now being used, even if it wasn't when they agreed to the terms and conditions?
    d. How do you balance your desire to be ethical and your desire to continue working at this company?
    e. What do you actually do to "fix" the issue?
B. Stakeholders
    a. Customers/users
        i. Data privacy/anonymity - more of an ethical right than a legal one, but you and the CTO care about maintaining your customers' privacy
        ii. Should be aware of how their data is being used - If you do start collecting data, users should be notified, as this may require a change to the terms and conditions
    b. Company employees
        i. Right to control how their app functions
    c. The local breweries
        i. They have the right to serve who they please. If, for whatever reason, the app makes running the brewery miserable, the brewery owners have the right to ban the use or users of the app in their brewery.
C. Missing information
    a. What have we been telling users about data collection/use so far?
    b. Can we truly "scrub" the data, if it's being logged in our web logs?
    c. Is it possible to collect *only* their location so long as they are at a brewery?
    d. How much power do the employees have over this decision?
        i. Can the CTO veto this kind of data collection?
        ii. Can *we* veto this?
D. Possible actions and consequences
    a. Argue with your boss/colleague
        i. Could potentially lead to them coming around.
            1. This could be them completely scratching the project, or else only coming to some intermediary compromise, in which case you still have to decide whether to compromise your morals.
        ii. Could lead to you being fired. Now nothing has been accomplished, but at least you tried. You could then decide to move on to option c).
        iii. Argue for an alternative solution:
            1. Have users volunteer their own information about where they've been rather than collecting it automatically.

        a. Still collecting data, but now totally voluntarily. No ethical concerns.
        b. Would collect far less data, and would probably get less accurate results
    2. Start tracking data, but don't use the old data that you told users you wouldn't track.
        a. If you're against all tracking, this is still an issue.
        b. If the announcement that the app is now tracking your movement is made crystal clear, the decision about users' data is now technically in users' hands—they can either continue using the app or delete it.
    3. Same as option 2, but give users the option to have their data tracked.
        a. Slightly fewer users may delete the app, since they are now given the option to not be tracked.
        b. Many users would probably opt out, meaning less data, and less accurate data (and thereby worse app performance).
        c. Ethical, so long as users are aware and informed about the decision they are making.
    4. Can be combined with other options: track only the fact that they visited a brewery, and no other location data.
        a. Not as lucrative
        b. Much more ethical
b. Resign in protest
    i. Almost certainly will not stop the company from harvesting/selling user data, but at least you're guaranteed that you won't ever have to go to work, actively going against your own morals.
    ii. You can still proceed to option c).
c. Anonymously "whistleblow"
    i. This may or may not solve anything, depending on your luck, and who you whistleblow "to".
        1. Alerting the rest of the company may make them protest, if they hadn't realized what was going on.
        2. Alerting the users of the app may be difficult, since it's unlikely you'd be able to communicate to them through the app, so instead would have to rely on typical news outlets. This may cause some users to stop using the app.
            a. However, not all users will see this
            b. This actively harms the company that you may still wish to work for
    ii. If you get discovered, there's the chance that you get fired.

iii. If in combination with option a) and b), you have essentially done all that you can, without actively harming the project, to prevent the unethical project from succeeding.

d. Actively sabotage the project
    i. This is unlikely to work, but has the chance to slow, or completely stop the progress of the unethical project.
e. Let the CEO and your colleague collect and sell as much data as they feel like
    i. Compromises your and the CTO's ethics
    ii. The CTO could possibly leave, which might lead to more sketchy behavior with less oversight
    iii. If users are notified of this, they will probably not be happy, and people might stop using the app
    iv. If you are not careful about the law, Beerz could face legal action
    v. More data for whoever is buying, which isn't actually anonymous

E. ACM Code Guidance
    a. Section 1.1 - All people are stakeholders in computing.
        i. As computing professionals, we have an obligation to promote fundamental human rights and protect people's right to autonomy. Selling their data (possibly without their knowledge or consent) would violate this principle. If we do want to sell data, it would have to be freely and knowingly allowed by the users.
    b. Section 1.3 - Be honest and trustworthy
        i. We must be transparent and provide full disclosure of the things we are doing. So if we wish to track and sell user data, we must disclose that to the users
        ii. We must not violate the trust of the users. The app has been running on the assurance that data is not being tracked or sold. To sell old data would be a violation of trust
    c. Section 1.6 - Respect privacy
        i. De-anonymization of data should be prevented - this could be done by scrubbing all location data except for the data that says "X person was at Y brewery on this day"
        ii. Unauthorized data collection/access - Again, we should not collect users' data without providing some notice. We must also take steps to protect the data we do collect, preventing hackers from getting into it

F. Recommended action
    a. We would speak with the CTO and come up with a plan for how to either prevent this project from being implemented as discussed, or else mitigate its negative effects. Based on that discussion, we would then probably go and talk to the CEO to make our case, as well as offer alternative solutions (see section D.a.iii.). We want to emphasize that selling data is an unethical idea and goes against our company and personal values.
    b. If the above does not lead to a result that we are happy with, we can always whistleblow to our users, and/or resign from the company.