

File name: misc/ethics.pdf

File owner: Lysander Miller

Collaboration: I brainstormed ideas with Kiri Salij

## ETHICAL ANALYSIS OF A SECURITY-RELATED SCENARIO

For this assignment, I will be analyzing the second scenario.

**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.**

Below are some of the ethical questions faced by the main character in the scenario:

- Should you help the company sell users' anonymized location data?
- Is selling Beerz's users' anonymized location data really that serious? How seriously would you be violating user privacy, if at all?
- A large number of corporations sell user data already. Would stopping Beerz from selling their users' data really make a difference? Or, would it just be a drop in the ocean.
- Do you personally have a responsibility to try to stop the company from selling users' data?
  - If so, do you have children, a spouse, or family members that are dependent on you and your income? Does your responsibility to them matter more than your responsibility to prevent the violation of Beerz's users' privacy?

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

Let's first discuss the CEO's relevant rights. It is the CEO's company and, thus, he has the legal right to make decisions regarding how the company uses the data it acquires. Additionally, although I'm not too well versed in data privacy laws, I believe he legally has the right to sell anonymized user location data.

Now, let's discuss Beerz's users' rights. While the users likely technically consent to their data being anonymized and sold, this consent is likely given when the user downloads the app and thus "agrees" to the app's terms and conditions. Do they have the right to be informed in a clearer way? Perhaps. However, would selling anonymized user location data legally violate users' right to privacy? I don't think so.

The main character in this scenario has the right to quit their job at Beerz. Additionally, they have the right to speak up against Beerz's CEO or, as long as they haven't signed some sort of NDA, they have the right to let others know what Beerz is doing.

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

Some questions that I'd like answered in order to make better choices:

- Can users opt out of their data being sold and still use Beerz 2.0?
- Will users know that their data is being sold?
- How much sway do you hold in the company? Would speaking up against the CEO make a difference?
- How financially secure are you? How much do you need this job? Do you have any dependents?
- Is Beerz dependent on you? Would leaving the company impact Beerz?

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

Some of the possible actions and their consequences are as follows:

- You could quit your job at Beerz.
  - Potential consequences:
    - If you're not financially stable enough to quit your job, this could have significant negative consequences for you and any dependents.
    - Someone else might take your place and implement Beerz 2.0 (with no data scrubbing) anyways.
- You could refuse to do the work to implement Beerz 2.0 until you were promised there would be no selling of anonymized user data.
  - Potential consequences:
    - If you're vital to Beerz 2.0's implementation, you might be able to stop the selling of anonymized user data. If you're not vital, you could lose your job.
- You could let Beerz's users know that Beerz will be selling their anonymized location data.
  - Potential consequences:
    - Beerz's users would stop using Beerz. Thus, their data would be protected from Beerz selling it. This could result in Beerz failing as

a company and result in everyone working for the company losing their jobs.

- Beerz's users would demand that Beerz doesn't sell their data. This could lead to Beerz not implementing their data-selling strategy. You'd also get fired.
- Beerz's users wouldn't care. People know that Facebook is selling their data, for example, and they still use it. In this case, you'd likely lose your job for nothing.
- You could just implement Beerz 2.0 without any data scrubbing. Or, in other words, go along with the CEO's plan.
  - Potential consequences:
    - You would likely feel guilty.
    - Beerz would raise their revenue. This could positively benefit you.
    - Because you helped out with Beerz 2.0, in the future, you might be able to either rise up within the company or gain more sway within the company. From there, you could try to convince others/make the choice yourself (if you've risen up to a role where you hold significant voting power) to stop selling anonymized user data.
- You could try to convince the CEO not to sell Beerz's users' anonymized location data.
  - Potential consequences:
    - If you hold enough sway within the company or make a persuasive enough argument, the CEO might decide not to go ahead with selling anonymized user data.
    - You could lose your job.

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

Let's now discuss the guidance provided by the ACM Code of Ethics and Professional Conduct.

Section 1.1 of the code says that "An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy." One could claim that, by selling Beerz's users' anonymized location data, Beerz is violating the privacy of its users. Thus, as a computing professional, the main character ought to be against Beerz's plan. However, one might also argue that Beerz's data-selling plan is, legally, not a violation of user privacy. Thus, not a concern.

Section 1.2 of the code says that “unjustified... disclosure of information” is a form of “harm” and, thus, should be prevented. While one might argue that what Beerz is doing is an unjustified disclosure of information, another individual might claim that users agree to disclose their information (specifically their location data) when they download the app. Thus, it’s justified disclosure of information.

Section 1.6 claims that “computing professionals should establish transparent policies and procedures that allow individuals to understand what data is being collected and how it is being used” as well as “to give informed consent for automatic data collection.” Once again, one individual might claim that users agree to disclose their information (specifically their location data) when they download the app. There is probably also some fine-print somewhere (in some sort of Terms and Conditions document) that users sign-off on. Thus, Beerz’s users would know what data is being collected and how it’s being used. Additionally, they would have given consent for their data to be collected. However, someone else could argue that this is not truly informed consent and the policies are not transparent.

Finally, section 3.1 states that “People—including users, customers, colleagues, and others affected directly or indirectly—should always be the central concern in computing. The public good should always be an explicit consideration.” While one could claim that Beerz’s CEO doesn’t have the public good in mind when proposing his data-selling plan, another individual could argue that selling users’ anonymous location data is not harmful to users.

Overall, it seems like the ACM Code of Ethics and Professional Conduct could help someone justify selling anonymous user location data or argue against such a thing.

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

Personally, I would recommend that the main character continues to work on Beerz 2.0 even if the CEO goes ahead with selling anonymized user location data. This is mainly because I don’t think that selling **anonymous** user location data is a breach of privacy. Afterall, what does it matter if some corporation knows that some anonymous person was at a specific bar at 12pm?

Additionally, even if I did think selling anonymized user location data was a breach of users’ privacy, I think that a large number of companies are already selling

users' anonymized location data. Additionally, Beerz is a startup and would not be selling nearly as much user data as Google or Facebook or other large companies. Thus, if Beerz was to sell anonymized user location data, it would, in my opinion, just be a "drop in the ocean."

Finally, I think that keeping one's job is more important than protecting the violation of strangers' privacy, especially if you have a family that's dependent on your income.