Varun Saini

Ethical analysis of a security-related scenario

For this assignment, I will focus specifically on Scenario #2, which concerns Beerz storing customers' personal data.

Ethical questions

Here are some important ethical questions that arise from this scenario:

- Is it ethical to extract and use old location data that wasn't originally intended to be stored?
- What is the right thing to do with users' location data?
- What responsibility do I play in this company in regard to upholding ethics?

Stakeholders' rights

Without further information about the laws within which Beerz operates, it is difficult to list every stakeholder's rights concretely.

Below are some rights for each stakeholder that I believe are fairly reasonable, but these details may vary depending on legal jurisdiction (imagine California laws vs. Minnesota laws).

Users

Privacy

Users should have the right to privacy over their location, especially if they haven't explicitly signed off on their location being stored on a server.

Informed consent

Users should have the right to be informed about how their location could be used before consenting. In addition, users should have the right to consent (or opt out) of their data being stored.

Data deletion

Users should always have the right to revoke their consent, even if they had previously granted it to Beerz. Consequently, users should be able to trigger a deletion of their data if desired.

Data download

This is less universally agreed upon, but users should have the right to view and download the data that Beerz has stored on them.

Senior executives

Profits

Senior executives have the right to establish and execute a business plan that maximizes profits for the shareholders of the company. As we see, the CEO is exercising this right.

Considerations (Profits)

Although senior executives have a duty to pursue profits, they must do so within the bounds of the law and must make ethical considerations. In addition, if the company has guiding cultural principles (for example, Google's "Don't be evil"), senior executives are also obligated to adhere to these.

Duty to the users

As representatives of the company's interests, senior executives also have the right to do what is best for their customers—this indirectly helps the company as well. Unfortunately, this leads us to murky waters: does the company know best, or does the user? In this situation, the CTO is most directly exercising this right by protecting the users.

Employees

Speaking out

Employees hopefully have the right to express their opinions about the company's business plan without retaliation. At the same time, if employees want to "remain professional" by being silent, they have the right to do so as well, even if they believe the company's plans to be ethically wrong.

Culture

Employees also have the right to help shape the culture of their company. If employees want to prioritize the goal of preventing surveillance capitalism, they have the right to reinforce this culture.

Information needed

Legal information

As stated in the section above, it is difficult to make decisions about the rights of stakeholders without specific information about the laws governing Beerz's decisions. This is especially true when considering legal implications, as these can vary drastically from state to state. I would want to know the relevant data privacy laws that apply to Beerz and whether they cover location-based information.

Data information

Crucial to this analysis is an understanding of what exactly is needed to enable the features in Beerz 2.0. After understanding this better, it might become easier to devise solutions that help earn the company profits but also protect users and their data.

Consequences

Depending on the laws and regulations governing data privacy, there may not be a significant punishment for what the CEO wants to do. This may be an incentive for the company to act in a profit-maximizing manner rather than in the best interest of users.

Possible actions and consequences

Annoying colleague's idea

If we were to proceed with implementing the annoying colleague's plan, we might be able to increase our revenue in the short run. Although there is a chance we never get caught, the risks associated with being caught are high. We likely would have violated a data privacy law, wasting time and money with legal proceedings. In the long run, this would likely hurt the company's profits and damage the company's reputation and relationship with users.

Scrub data after one week

Assuming that this is implemented with the appropriate checks in place, this approach has privacy-related benefits. These checks would ideally require users to consent to their data being stored for one week and give them the option to request the company to delete their data. Users would also be able to revoke their consent at any time. At first glance, this approach seems like it would reduce profits, as the company wouldn't be able to sell historical location data. However, it is possible that preventing legal fees would save money in the long run.

Create a new opt-in privacy tier

In this scenario, we can do the same as described in “Scrub data after one week.” In addition to this, we could create a new opt-in privacy tier for users who are okay with their location data being sold. As long as users are made aware of these plans and certain safety measures are implemented (like anonymity and adding “random noise” to the location data to make it less exact), the company could sell these users’ location data without serious privacy concerns. Although this approach would take longer to ramp up than the annoying colleague’s idea, it would be safer from a privacy perspective. This approach is promising, as it still supports the CEO's dream of selling location data, but it does so in a way that is more compliant with the law.

Guidance from the ACM Code of Ethics and Professional Conduct

The following principles from the ACM Code of Ethics and Professional Conduct are relevant to this situation.

- 1.2 Avoid harm.
- 1.3 Be honest and trustworthy.
- 1.6 Respect privacy.
- 1.7 Honor confidentiality.
- 2.2 Maintain high standards of professional competence, conduct, and ethical practice.
- 3.1 Ensure that the public good is the central concern during all professional computing work.

As illustrated by these principles, the decisions we make must respect the privacy of our users, avoid harming them, and honor their confidentiality. Even if we do choose to sell location data, we must be transparent about this decision and be extremely careful about protecting our users in the process. Finally, it is the responsibility of employees to uphold the company’s ethical duty to the public good. Employees must step up and prevent the company from making unethical decisions.

Recommended action

Description

Implement the plan described in “Create a new opt-in privacy tier” above.

Justification

Both the CEO and the CTO agreed on the basic plan for Beerz 2.0, so it makes sense to implement that. Appropriate privacy measures have already been put in place for that plan (data scrubbing after one week). In regards to the CEO’s plan to sell location data, this is not

inherently an unreasonable or unethical goal. The annoying colleague's suggestion, however, is extremely unethical, as it goes behind users' backs and undermines their opt-out rights. That suggestion should not be implemented. However, by informing customers about the company's plans for their data and providing users the ability to opt out, these concerns are lessened. To further prevent ethical issues, we could also still implement a long-term data scrubbing process for individuals who consent to their data being sold, say, once a year.

Answers to ethical questions

Is it ethical to extract and use old location data that wasn't originally intended to be stored?

No. This is unethical because users have not consented to it. This could also potentially tarnish the reputation of the company.

What is the right thing to do with users' location data?

The right thing to do with users' location data is to keep it safe and anonymized. It is also our duty to store it for as little time as possible to prevent potential security risks. The longer we store this data, the greater the chance that it gets into the wrong hands. Finally, it is also our duty to inform users about how their data is being used and give them the option to have it deleted from our servers.

What responsibility do I play in this company in regard to upholding ethics?

It is my responsibility as an employee of the company to ensure that the company is acting ethically. As stated in the ACM Code of Ethics and Professional Conduct, I must "[e]nsure that the public good is the central concern during all professional computing work."