McKenna Wirth and Antonia Ritter

CS338 Spring 2022

ETHICAL ANALYSIS OF A SECURITY-RELATED SCENARIO

We will be working with scenario 2 (Beerz customers' personal data) for this assignment.

Main ethical question

Should you take action? Selling data is technically legal, although it is morally questionable to you. Therefore, you need to weigh the moral costs with your desire to remain employed.

Is finding, using, or selling past user data (i.e. Beerz 1.0 data) worse than beginning to collect that data? How much worse? We would question the legality of this as well as the morality, based on the terms of service that users agreed to- if they did not consent to the collection of their data, then it would not be allowed.

Stakeholders and their rights

You- The right to continue or end your employment as you see fit and act in your own self-interest, be that by keeping your job at the expense of someone else or by leaving to spare yourself moral anguish.

Users- The right to not have their data recorded or sold without their knowledge; perhaps the right to not have their data recorded or sold.

Company management and shareholders- The right to operate their company as they see fit within the law; the right to act in the interest of the company/profit.

Data brokers- The right to operate their business to the extent of the law, or to operate their business to the extent that is moral, depending on your perspective.

Breweries- The right to advertise their business in any legal ways they want.

Additional information

Feel out the CTO for her real position (given that there's evidence she's not happy about it). How influential is she in the company? Are there others that share your/possibly her perspective?

Do the web logs containing the GET requests with user location data ever get deleted? How are they stored/protected?

Did Beerz 1.0 promise users that their data wouldn't be saved?

Can we get that annoying dude fired?

How is the company's financial situation? Are they interested in selling user data because the start-up is on the verge of financial collapse?

What specific information is collected? How detailed is it? Does it include all location data or just brewery visits?

Can you easily get another job?

Do we expect that any harm will come to users after their data has been sold? Do we have any agency over who that data is sold to? Is this data that they aren't already giving away to other services (maps apps, etc.)?

Actions and consequences

Talk to the CTO, CEO, and other people involved and express your opinion. Hope you're not fired over it. This may change their minds, which would be great and resolve the situation entirely (though maybe you should also get them to delete the web logs). Or it may not- money is a powerful motivator. As communication is often the best approach, this is a good starting point.

If they persist in this course of action…

Continue to do your job. There wouldn't be any consequences for you, unless you count guilt, but any harm from sharing their data would still fall on the app users.

Quit. This wouldn't help the app users at all, but you wouldn't be complicit.

Lie and say that you can't get the system to work. This might eventually get you fired or demoted and, as there are other engineers, would not solve the problem. Also, people might start thinking you're kind of stupid. However, it's still technically an option- albeit a bad one.

Leak the story to a journalist. This is a very risky option- start your job search now. The company is likely fairly small, so the odds of you being identified as the source of the information are fairly high. If that happens, you would most likely be fired, but you might spark a renewed interest in this debate- people who visit breweries constitute a sizable proportion of the voting public and could be very vocal if their beer is implicated.

Plant code in the app that alerts users to the scheme to sell their data. Bonus points for a fun graphic! While this would inform users, and those who continued to use the service would therefore have been able to consent with this information, you would likely lose your job and we don't think Beerz would be willing to act as a reference for you.

ACM Code of Ethics and Professional Conduct guidance

Principle 1.3, "be honest and trustworthy," rules out a few of the options above, but they weren't good options anyway.

Principle 1.6, “respect privacy,” encourages you to speak out against the selling of user data, particularly that from Beerz 1.0 where users may not have consented to their location data being collected in the first place. This would mean you shouldn’t simply continue working there or quit without voicing your concerns.

Principle 2.2, “maintain high standards of professional competence, conduct, and ethical practice,” rules out a few of the options above that would violate professional norms.

Principle 2.7, “foster public awareness and understanding of computing, related technologies, and their consequences,” endorses some of the options that involve educating others on the possible negative outcomes of selling user data.

Principle 3.1, “ensure that the public good is the central concern during all professional computing work,” may be violated by the proposed plan to sell user data, speaking to the importance of this ethical dilemma.

Recommended action

We recommend the first action discussed: talking to your coworkers. There are better and worse ways to do this, and it would probably make sense to talk to potential allies (like the CTO) first, then find a compelling way to present your case.

If this works and you convince them, great. If not, you have to decide what to do. The sensible courses of action are either quitting or continuing to do your job. Decide how immoral you find the situation (perhaps more if they sell Beerz 1.0 data) and whether you can in good conscience participate (the last three questions in the Additional Information section are relevant here).

In judging the level of harm, note that people who frequent breweries are not a particularly sensitive population. There is no stigma around visiting these establishments and people who can do that regularly are likely to be of a higher socioeconomic status. That said, if the location data is more than just visits to specific breweries, the potential for harm increases.

With respect to our second main question (is selling Beerz 1.0 data more unethical), it would be nice to have some additional information about what the users agreed to and what the data is. Regardless, the users likely had not agreed to the sale of their data at that point in time, and they do not have the opportunity to stop it, so we find this less moral. In the US, you cannot create retroactive laws. This example is a similar situation.

This discussion of ethics could continue into perpetuity. The ACM Code of Ethics provides some helpful guidelines, but many of these decisions must be made by individuals, making use of their own moral code. There is no one perfect answer, so all we can do is try our best.