SCENARIO #2: YOUR COMPANY'S CUSTOMERS' PERSONAL DATA

In Scenario #2, we see an example of a company approaching an ethical crossroads around the responsible use of user data. As an employee, we joined this team in part because we identified with its privacy-oriented mission: to provide relevant brewery information to users without abusing momentary access to their data or putting them at risk. Now that the CEO seems to be on board with another employee's idea to store and sell user data, the integrity of that mission is in jeopardy. It's a situation that seems like it could turn unethical quickly, especially if users have limited knowledge or control around the sale of their data. We are keenly aware of this danger, but we are also surrounded by co-workers we like, a comfortable working environment, and a steady job. So the question is, how will we choose to act? Should we quit on principle? Should we keep our mouth shut and hold on to our job? Should we try to persuade the CEO to take a different route? Or is there some other option?

In order to make an informed decision on what an appropriate course of action would be for us in this position, we can begin by assessing who the different stakeholders in our situation are. By looking at all the possible stakeholders, we will be able to see both how our action may end up impacting each of the relevant parties and what available courses of actions are within the confines of the rights of the stakeholders. The first, and perhaps most obvious stakeholder in this situation would be ourself, the employee. As an employee, we primarily have the right to stay and continue to work at Beerz or quit our job. Further, we have the right to free speech, which entails speaking up for our ideals (although this comes with its own constraints that we will discuss later). Another stakeholder is the company. In most states, the company has the legal right to sell customer data without informing the customers in question. Further, it has the right to take actions against either current or former employees whom it finds in contempt. For example, Beerz may fire a current employee for pushing the idea that the company should not sell customer data, or sue a former employee for spreading word that Beerz sells customer data. The last relevant stakeholder in our situation is the customers themselves. Ethically speaking, the customers **should** have the right to know when their data is being sold and what kinds of data is being sold. Also, the customers have the right to stop using the Beerz platform if they should feel the need to do so.[1]

Alongside the discussion of rights by the major stakeholders, there are a few areas of ambiguity in the scenario that could influence the correct course of action. For one, would the Beerz app give users the option of whether or not to offer up their data? The phrasing of our annoying coworker sheds some doubt on this, but ultimately this distinction is up to the discretion of the CEO and other higher-ups in the company. Assuming that data collection is not optional, would the app disclose to users that it is collecting their data, prior to use of the app? If so, how obvious would it make this fact? Apps and websites take a wide variety of different approaches to user consent and policy disclosures. For example, many websites will promptly display a banner disclosing their use of cookies upon loading the site. Some will allow users to

[1] In a similar vein, our deeply annoying and profoundly clueless development colleague has the God-given right to remain silent during company meetings.

accept or reject cookies, or even to select which specific cookies they consent to. But many more will also employ unscrupulous methods to make their cookie messages confusing, annoying, or otherwise disingenuous in ways that take advantage of the user and increase rates of cookie 'consent.' In the same vein, the Beerz app has any number of options available to them in regards to user consent and disclosure, between not asking at all, hiding it in their terms of service, making the app unusable otherwise, and fully giving users a choice. Another area of ambiguity that could influence our potential actions is what share of location tracking data Beerz would contribute if it decided to sell customers' data. If it would comprise an extremely small amount of available location data (compared to other apps, like Facebook or Instagram for example), the harm being done by the company may be relatively small enough that the benefits of working there—e.g. job stability, whatever utility the company offers to the world—outweigh the consequences. Finally, there is the question of how the app would be making money outside of the potential sale of user data. Do users pay for the app itself? Is it free, with available micro-transactions to activate additional features? Does the app show ads? If brewery location services are provided for users in direct exchange for their data (and this is made clear to users), perhaps this model could be considered ethically sound.

After having considered the rights of the stakeholders (importantly of ourselves, the Beerz employee) and some information that might help educate our decisions, we can move on to considering some possible courses of actions that we can take in light of the situation. One action that we can take is offering the company an ultimatum: either cut the crap about selling customer data, or we will leave the company. While this is unlikely to be effective (Beerz has its sights on the skies), it is within the realm of our rights and would possibly relieve us of culpability for the infringement on users' rights (although it may be that we are haunted with the guilt of not doing more for protecting customers' privacy by springing this ultimatum on the company). Another action we can take that may protect customer privacy is by leaking information about Beerz's nefarious plans to a media outlet. After the information is released, the customers may then exercise their right as stakeholders to stop using the service and in doing so, help protect their own privacy. However, we run the personal risk of prompting Beerz to pursue legal action against us, as is within the realm of their rights; this undesirable outcome would be a massive disutility to ourselves. A slightly different action that we can take is to simply allow the company to sell users' data. As we mentioned in the prior paragraph, it may be the case that the amount of harm that Beerz would cause in selling users' location data contributes to the total pool of location data so little that it would be negligible. In this case, the value of Beerz getting more profits may outweigh the small cost of incurring negligible privacy infringement on the customers (remember also that the batch of location data up for potential sale is anonymized). A final course of action is staying within the company, and attempting to persuade our co-workers and CEO against selling customers' data. It is important first of all not to make assumptions about what people want. Clearly, the CEO is excited about the potential profits from selling location data, but perhaps they have actually failed to consider the ethical ramifications, rather than acting in bad faith. Regardless, there might be some amount of leeway available in at least

floating these issues to the CTO, who can in turn communicate with the CEO at her own discretion. Speaking directly with the CEO is also an option, of course. Though neither of these options is guaranteed to yield a compromise (and could have an effect on our job security), they might be actions worth taking.

Having discussed our possible courses of action, we can look to the ACM code of ethics for some guidance on how best to determine our course of action. The ACM code of ethics states that we should "Ensure that the public good is the central concern during all professional computing work" (Section 3.1). In other words, our focus turns to the question "How can we avoid harm and maximize public good for our customers?". If we consider the option of simply allowing the company to sell customer data, under this light, we can see that this outcome is flawed. While it may be that Beerz gets more relative utility out of selling customer data than the disutility that comes to the customers themselves, the ACM makes clear that we should not be prioritizing Beerz's gain in the first place. The "public good" comes first and foremost, and as such we should exclude Beerz's profit from our moral decision-making process. Other relevant sections from the ACM that can help inform our decision are sections 1.3: "Be honest and trustworthy" and 1.6: "Respect privacy". In our particular situation, these sections would require that Beerz inform the customers about its decision to sell their data. More specifically, if we were complicit in Beerz's decision to sell user data, we would need to make a concerted effort to educate the customers on what the selling of their privacy means. It would be simple to slip a section about consent towards selling customer data in a Terms of Service document, but in order to properly adhere to the ACM we would need to go a step beyond and make sure that the customers understand what it means to have their location tracked.

After having reviewed the possible courses of action and how the ACM can help inform our decision-making framework, we can finally come to a decision on how to properly proceed with our situation at Beerz. We believe that the best course of action to take is to stick with the company and continually make efforts to maximize the public good in any way we can. We noted earlier that drastic measures, such as offering the company an ultimatum or going to a media outlet about the situation, are available to us. However, because our scope of influence is going to be limited, we want to choose a course of action that will bring about the most good in the long run. Because the company may be protected by the law, it seems that these more drastic options are unlikely to end up in the customers' benefit in the long run. Instead, staying within the company and making constant efforts in the interest of public good is a reasonable way to ensure at least some degree of success. For example, we may start off by attempting to educate our colleagues and bosses about the importance of customer privacy and persuade them to not sell customer information. However, even if that fails, we have other areas of recourse. We could, using our position as a developer of the Beerz app, make it exceedingly clear to the customers that their location data is being sold and what that would entail. Putting ourselves in a position to maximize public good within a company seems, to us, to maximize the expected value of benefiting the public good.