Author: Kyle Machalec

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

A.

In scenario #2, we are part of a company that is deciding how to handle user data. We decided to join the company partly due to the CTO's pitch that the company protects its users' data while it has it and discards the data when done with it. The CEO has decided to threaten that mission by pushing for storing and selling user data. The situation could quickly turn unethical, especially if the users are not clearly informed of the company's policy changes or not in control of how their data is used. We like our job, we love nearly all our coworkers, and we believe in the vision that the CTO shared. However, now we need to decide how to react to the CEO's proposed changes. Should we act behind the CEO's back and leak these new policies to the public? Should we just quit the company and leave this issue behind? Should we try to persuade the CEO to change their mind? Or is there some other option?

B.

To begin to understand what course of action is best, we must first consider the different stakeholders in this scenario. It is important to consider how our actions can affect each stakeholder and what actions each stakeholder can take within their legal rights. The first, likely most obvious stakeholder is ourself, the employee. As an employee, we have the right to continue working at Beerz or quit our job (although we may have to face certain penalties if we are under contract). In addition, we have the right to free speech, which involves speaking up for our ideals. Another stakeholder is the company. In most states, companies can use, share, or sell any data they collect about you without notifying you that they're doing so. Furthermore, companies have the right to take action against any current or former employee whom it finds in contempt. For example, a company can fire an employee for acting against the company's decision to sell user data and can sue an employee for spreading the word that the company sells user data. The final relevant stakeholder is the customers that use the Beerz app. The most important right a customer has is the right to stop using a service should they decide it no longer offers what they want. Of course, a customer would only be able to decide to stop using the Beerz app if they were aware of the disagreeable policy changes (which they may not necessarily be entitled to as stated previously).

C.

Before considering the merits of potential actions we could take, it is useful to identify missing information from the scenario that could influence our decision. For instance, it is unclear whether Beerz gives users the option to choose how they want

their data handled. Furthermore, it is unknown whether Beerz intends to notify their customers about the change in how user data is stored and shared. Even if Beerz notifies its customers about the policy change, we don't know how clear this notification would be (the notification could be fine print hidden within a massive legal document). Finally, it is important to consider how the app makes money outside of selling data. Do users have to pay an upfront fee to download the app? Is the app free with additional paid features? Are there any ads? If the app is free, and the company makes it clear that users are exchanging their data for Beerz's services, then Beerz's decision to sell user data could seem ethical.

D.

There are numerous ways we could respond to this situation. One way would be to leak information about Beerz's plans to the public. If Beerz's users understand how the company is using their data, they can make informed decisions about whether or not to continue using the app. However, this action runs the risk of Beerz taking legal action against us if they can trace the leak back to us. Even if Beerz does not win the legal battle, it would still cost us time and money to defend our case. A different action we could take would be to make an ultimatum: if the company chooses to implement the CEO's plan, then we will quit our job. Unless we are a particularly influential employee within the company, our threat to quit is unlikely to alter Beerz's plans. While no longer an employee of Beerz, we could avoid any responsibility for Beerz's future decisions, but we would have to deal with the guilt of having done nothing to protect user data. The opposite action we could take would be to just simply continue working at Beerz without taking any special action. If the media got wind of Beerz's shady policies, the leaders of the company like the CEO and CTO would likely get most of the attention, and you could slip under the radar. However, just like quitting the company, you would have to deal with the guilt of having done nothing to prevent this issue. One last action we could take would be to try to convince the CEO of the value of data privacy. The CEO is clearly excited about the prospect of making money from selling user data, but they might not have considered the ethical ramifications of getting that extra money. In this case, the CEO could be open to reason. Of course, depending on the personality of the CEO, challenging their beliefs may have consequences for our job security. If the CEO disregards your concerns, you could respond with any of the other previously mentioned actions.

E.

Now that we have considered many courses of action, we can now look at the ACM code of ethics to help us determine which action is best. Section 3.1 states that we should "ensure that the public good is the central concern during all professional computing work." Taking this into consideration, we can see that the choice to just

continue working without taking action is flawed. According to this section, the “public good” takes priority over all other matters, including the company’s profit that could be obtained by selling user data. As such, it would be irresponsible to make no attempt to correct the company’s profit-driven data management plan. In addition, section 1.3: “Be honest and trustworthy” and section 1.6: “Respect privacy” prompt Beerz to clearly inform its users about how their data is being used. This further emphasizes the need for us to take some kind of action to steer Beerz away from secretly selling user data.

F.

After having reviewed the possible actions and the ACM code of ethics, we can come to a decision about how to handle the situation at Beerz. It appears like the best course of action is to stay with the company and try to convince the CEO to either not sell the data or sell it only after informing users about this change. Continuing with working at the company without taking an extra action is irresponsible according to our discussion of the ACM. Furthermore, drastic action like quitting our job of leaking information to the media may not help the company’s users in the long run. Once we quit our job or get fired, we lose much of our ability to influence Beerz’s data management policies. In addition, becoming known as someone who leaks company secrets could be detrimental to our own career. If we stay with the company, we can share our opinions with our coworkers and the CEO in the hopes of sparking discussion about the moral implications of selling and storing users’ data. Even if this fails, we could, as a developer of the Beerz app, help make clear messages that inform users about how their data is being used and what that entails. By sticking with Beerz and guiding its actions from within, we would be in the best position to ensure that the public good is kept as the company’s central concern.