Ethical Analysis of a Security-Related Scenario
Author: Ashok Khare
Chosen Scenario: Scenario 2

The main ethical question in this scenario is whether or not to go along with the plan to store and retrieve prior user data in order to sell it in the future. If we decide not to go along with the plan, there is also a question of whether to report it to legal authorities, or to just refuse to work on the project. The real consideration behind these questions, though, is whether or not the proposed plan is ethically and legally acceptable. For this writeup, we will assume the setting is in the United States.

The most important category of stakeholders in this scenario are the users of the service. For this group, we must examine rights regarding sale of their personal data. According to the ICLG's article on active data protection laws in the United States in the years 2021-2022 (found at https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa#:~:text=There%20is%20no%20single%20principal,Code%20%C2%A7%2041%20et%20seq.)), although there is no supreme national legislation regarding user rights in regards to data protection, there are several regional statutes and state regulations that are designed to protect the sale of user data. An example of this is Utah Code 13-37-201 (found at https://le.utah.gov/xcode/Title13/Chapter37/13-37-S201.html), which states that commercial entities seeking to disclose personal information to a third party for the purpose of compensation must provide a specific notice to the user whose information is being disclosed. Thus, while there appears to be no de facto prohibition on the sale of user data, there are several pieces of legislation that require companies to notify and acquire permission from users before selling their data to a third party.

Another category of stakeholders is the Beerz 2.0 company itself. The rights of this group are closely connected to the rights of users. As the company is trying to sell data solely to generate additional revenue, it must abide by laws that require it to notify users of data disclosure, as well as provide an option to opt out of data disclosure entirely, in accordance with policies such as the California Consumer Privacy Act (CCPA, whose stance on the sale of data can be found at https://oag.ca.gov/privacy/ccpa#sectionb). Otherwise, there is nothing legally prohibiting Beerz 2.0 from selling user data.

A final category of stakeholders is the buyers of the data being sold by Beerz 2.0. There does not appear to be any legal prohibitions on the purchasing of personal data in the United States; for the most part, the restrictions on the personal data economy seems to be focused on restricting sale. In this context, there is no legislation blocking the purchase of personal information by third parties, as long as it is allowed to be sold.

Although the given scenario seems straightforward for the most part, one clarification that I would appreciate centers around the design of the API. The development colleague mentions that the API archives web logs, which contain user information. If the archiving capabilities were specifically added by the developers at Beerz, that would entail significant ethical and legal violations. If this were the case, the CFO's claim about discarding user data

when the company is done with it would be a lie. This raises the possibility that Beerz is actively misleading its employees and customers regarding its data use and storage policies, which would undoubtedly carry legal consequences. However, if the archive functionality of the API is out of the control of the developers - i.e. they did not create it and have no means of removing it - then, as of yet, the company would not be misleading its employees and consumers. If it started keeping track of archived data but maintained its claims of discarding user data in a timely manner, then there would be moral and legal trouble. But as long as the data is actually being discarded and the developers are not personally responsible for the existence of the API archives, then the company is not technically engaging in any false advertising or other illicit activity.

In this scenario, I could take several courses of action. The first possibility would be informing legal authorities of the company's intentions to shut down the operation entirely. However, this seems like an overly hasty decision, and would probably have severe consequences for my position on the team. The only instance in which reporting to the authorities would pay off would be if the company went ahead with data sales, but didn't adhere to the requisite statutes such as those mentioned earlier. If customer data were to be sold without the customer's knowledge, and without their ability to opt out, that would certainly be a legal breach and worth reporting to legal authorities. However, if the company was willing to follow the appropriate legislation in providing notices of data use and opportunities to opt out, then reporting the situation would not only be pointless but would threaten my position at the company. If I needlessly reported Beerz to the authorities, it is entirely possible I could be penalized with demotions or even let go as an employee.

A second course of action would be allowing the company to go through with its plans. The risk in this case is that I would be complicit if the company did not adhere to the appropriate legislation. Thus, the company (and perhaps even myself as the developer) could be subject to lawsuits and other penalties, which may even include being forced to shut down the service entirely. However, if all the appropriate legislation were followed as described above, then myself and the company would have nothing to worry about, and would be able to pursue the plan as desired.

A final course of action would be to refuse to work on the service, but not report it to the authorities. This is probably the worst decision out of the three. As a consequence of refusing to work, I could reasonably be demoted or fired, threatening my relationship with the company. Furthermore, since I had knowledge of the project but did not report it, I might be labeled as an accomplice in any legal breaches resulting from disregarding the aforementioned legislation. Thus, not only would I face consequences in the company, but I would also have to deal with the legal consequences of breaking data protection laws.

The ACM Code of Ethics (found at https://www.acm.org/code-of-ethics) provides a couple points that offer useful guidance. The points in question are 1.3 and 1.6. Point 1.3 advises honesty and transparency when describing a system and its capabilities, and not making false claims about a service or technology. Point 1.6 emphasizes using as little personal data as necessary in a service, and making sure consumer rights are followed. Furthermore, it specifies

the responsibility to inform consumers if their data will be used for any purposes beyond the original. Considering these points in the Code of Ethics, I feel that it is legally and morally the right thing to do to inform users of how exactly we plan on using their data, and giving them the opportunity to opt out of having their data collected if they do not agree with our terms.

Overall, I think the best solution for this scenario would be to go ahead with personal data sales, but be sure to include several visible notices and options in the service. Firstly, the service should display a notice detailing what the company does with users' personal information - that it is first used as advertised in the app, and then is saved and sold later. Then, the system must also include an option for users to opt out of sending their personal data to the company to use and store. Although this would mean that those customers could not make use of the 'find nearby breweries' service, they could still see popular breweries based on data collected from other customers who were willing to let the company collect, use, and sell their location data. With the data use notice and opt-out policy in place, though, it is totally reasonable for the company to collect and sell the data of consenting users, since the enterprise is within the bounds of the legislations and guidelines mentioned earlier in the writeup.

To be fair, the ethical issues of selling personal data are sticky. Personally, I believe the core consideration when determining the morality of data sale is the level of control consumers have over the process. If customers are unaware their data is being sold, or if they know their data is being sold but have no means to control or stop the sales, then the service is undoubtedly immoral and in the wrong. However, if customers (a) are informed by the service exactly what their data will be used for and (b) able to rescind permission for the company to sell their data at any time, then data sale is more acceptable, as the customer has full consent and control over the situation. Importantly, the customer must continue to have this total consent and control as long as their data is in the company's system. If either of the aforementioned rights are violated, or the company somehow otherwise prevents the user from controlling how their data is used, then the use of that data is once again immoral and the company is in the wrong.