Devin Lewis | CSS 338

Scenario #2

In this scenario we're faced with a young company that's creating an app based around the location of its user, so right off the bat it's obvious the main questions and concerns would be based around user information and their privacy. The main question here is is it ethical for the company to sell user location data for money? Other questions like:

- Would they have to communicate with their users that they're now using their data?
- Are they allowed to go back in their web logs to sell the data of prior transactions using their app? Transactions made where they already promised their data would be deleted
- Is it ethical for the company to even still have access to old API web logs?

All of these questions and more are likely what we're dealing with here.

Involved in this scenario are three main stakeholders that all have influence over the data in question in one way or another. First is the company Beerz who has the rights over its app and the usage of it, including the code used to construct it and trade secret rights with respect to the functionality and development of the app. Then there's the user who has the rights to any part of their data and privacy that they haven't already made an agreement on, and also the right to know of any major changes to a service they're using. Lastly there's also the data collectors, that is to say the people who would potentially obtain the bundled anonymized location data from Beerz. They aren't that relevant with the prior questions but they are worth acknowledging, and it's worth noting their right to use and store the data given to them if the transaction happens.

In fact, something that is important but wasn't really brought up in detail was exactly WHO this 3rd party is that wants to pay for Beerz's user data. Depending on who it is, it does change how serious this transfer of private information is. What's more, we don't know who in the Beerz company has access to these logs, is it everyone? Is it only a specific division? If it really is just open to anyone at that startup then that's already a big security risk by itself.

Even with the lack of information, there are a few paths we can take with this scenario. The first would be to talk to our boss and convince them to not sell the user data at all. Not only was this one of the main motivators for why you joined the company, but also it's clear that this is a violation of rule 3.1 in the Code of Ethics where computing work should be done for the public good, but here it's clearly only a change for company income. The only real consequence of this would be a potential source of income for the company, but nothing else

The second option would be to go through with the plan, but at the very least let consumers be aware of the change you're making to the service. Either through contacting them, putting an update message, or even updating the terms of service agreement, it's important to at least let users know that their data will be used and collected. While you will lose some of their trust with this change, now you can with a somewhat more clear conscience send their data since at least now you know they consent to it.

The third option, and the worst option, would be to go along with the plan and begin selling user data secretly without their discretion. This is highly unethical and basically illegal, but larger companies like Facebook and Google have done this to their customers before and more or less got off the hook for free, so maybe it'll work here. The only consequences though would be if you were exposed, then all your customers would lose faith in you, you'd be prone to several lawsuits, and since you're only a startup you'd likely go out of business. Worth a bit of extra cash though right?

Well let's take a look back at the Code of Ethics from before, and we'll see that the third option is 100% not the correct choice. Not only does it clearly violate rules like 1.6 which is to respect user privacy, but also 1.3 where you need to be honest with your consumer about all the details of the service you provide. It also violates 2.7, where the company has the responsibility to give the public awareness about the technical knowledge behind the scenes, including their access to the API back weblogs.

Therefore I believe that the best option is the second one, which may be surprising at first but you need to look at it from a business perspective. Sure you're still selling user data, but now you're doing it with consent which no longer violates any of the rules in the Code of Ethics, and since you're a startup being able to make any monetary gain is important if you want a chance at becoming a sustainable company. Maybe one day, you'll even be sustainable enough to no longer need to sell user data! However one important thing to note is to still scrub the data once it becomes a week old, AND to not allow common access or sell anything from the API web logs. The reason for this is to keep consistency and honesty to all customers using the service, but if you use data from users who did not consent to having their data sold then you once again are breaking the Code of Ethics.