Ethical Analysis

Peter Kelly

October 24, 2023

A. In scenario 2, the question of what to do after your meeting is the ethical problem. This response could be wide and varied but likely involves talking to someone, most likely the CTO, CEO, or the media. There are other ethical implications to consider, especially when a startup's negative reputation could directly cause layoffs.

B. Here the stakeholders are you, Company Employees, the CTO, the CEO, and the public. You have a right to create a work product that does not conflict with your personal values and also a right to speak out against deceptive capitalist surveillance. The company employees have a right to not be punished for a problem they did not create. The CEO has a right to make business decisions which they believe help their customers and employees the most. The public has a right to be told the truth about how their personal information is used, and a right to not have data which they did not agree to be stored to be used.

C. I would want to know a lot more about how the location data is anonymized before I made any decisions on this topic. In large cities with many users, if the data could be obfuscated enough that individuals could not be identified from the data it may be more acceptable to sell this type of data.

D. To me, the easiest action would be going to the CTO and voicing your concerns. This gives the CTO some support when they try to talk to the CEO, and will hopefully force that conversation. This could be a large personal risk to the CTO, especially if they are not on good terms with the CEO. That also creates a risk for the CTO to say they would talk to the CEO about it but then never do. You could also go directly to the CEO. This could be a personal risk for you but it could also reflect poorly on the CTO since you felt in necessary to go over their head. Finally, you could also go to the media. This has huge potential consequences for you, the company, and the public. If the company took a loss, it could result in the loss of jobs and a reduction in the service provided to the public. Yet either way, you are likely to take a personal loss as few companies are sympathetic to journalist's sources.

E. The ASM provides guidance for how users should be treated. Section 1.2 states that ”A computing professional has an additional obligation to report any signs of system risks that might result in harm.” and ”the consequences of data aggregation and emergent properties of systems should be carefully analyzed.” This implies that you would have a responsibility to report your concerns to someone. Yet it also states that ” computing professional should be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties.” So, even if you were to determine that the location data could be safely collected going forward, you would also have a responsibility to notify the customers that their data had been stored in a potentially compromised location when the location data was incorrectly kept in the url logs. Finally, it states that aggregated, anonymized data can be used but ”requires taking precautions to prevent re-identification of anonymized data or unauthorized data collection, ensuring the accuracy of data, understanding the provenance of the data, and protecting it from unauthorized access and accidental disclosure.” It also has guidance for professional relationships. In a healthy workplace, the ASM 2.4 says that you should ”Accept and provide appropriate professional review.” This means that you should provide feedback to the CEO or CTO if you believe that it is needed.

F. I believe that the correct course of action is to go to the CTO and voice your concerns and ask for further information on how the data would be treated and used. This follows the guidance that you should provide professional feedback. Yet, even if you do not learn how the data is being protected then you should check if they are using data that they did not initially notify users that they would use. If they are and are unwilling to tell the public, you may have a responsibility to inform the public that their data is being misused. No matter the outcome of the first two parts, you would also have a responsibility to ensure that the public is notified that their data was stored in an insecure log of URLs where their location data was visible in the GET parameter. Throughout the entire process you have a responsibility to minimize all harm, and this may prioritize customers' rights over the company's well being. Yet, you also have a responsibility to minimize harm to the companies employees. This means you should be as careful and diligent as possible before revealing information that could damage the company and hurt peoples' lives as there is the possibility that you could be wrong.