Personal Data Ethics

Transitioning from Beerz 1.0 to 2.0 has led to many problems related to data security and data ethics. Most notability historical location data of its users. The company initially followed a strict data policy where all location data is removed from storage following computation. Effectively protecting user data from leaks and marketing as all location data is deleted. In transitioning from 1.0 to 2.0 it is now a requirement to keep a week's worth of location data. With this change, the company can still keep its data privacy stance. After a week this data is deleted protecting historical user data, although with slightly more risk holding due to holding a week worth of historical data vs a single day. This change is still inline with the company's data privacy stance and the users assumed data privacy. This additional data store only increases data risk minimally while also increasing the value and usability of the app, a fair trade to make. Although demands from the CEO stand in direct contrast to the assumed stances of the company. Storing all new information as well as recovering past information not only changes the direction of the company but violates assumed user privacy.

First, it is important to understand the rights of all the parties affected by this change.

- Users have the right to privacy, informed consent, and control over how their data, especially sensitive information like real-time location, is collected, stored, and shared. Any decision to recover old data or extend retention without their explicit consent would violate these rights and breach the trust established in the original user agreement.

- Developers and engineers, including myself, have the right and responsibility to act in accordance with professional ethics and to refuse directives that would compromise user privacy or violate company policy. We are also entitled to transparency about how our work will be used and to be free from retaliation for raising ethical concerns.
- The CTO has a right to ensure that company policies align with its founding vision and that technical implementations remain consistent with user expectations of privacy.
- The CEO and upper management have the right to explore new business opportunities but are bound by their duty to honor commitments made to users and stakeholders regarding the handling of data.
- Investors and other stakeholders have a right to honest communication and consistency in company values. If Beerz shifts from a subscription service to data monetization, stakeholders should be fully informed since it changes both ethical and financial risk.
- The public at large also has an interest in responsible data handling. Privacy breaches or unethical data sales can undermine public trust in digital services generally.

The company's practices involving sensitive user data such as location are most certainly in writing in user and stakeholder agreements. Regarding the user policy, recovering and storing data could be grounds for legal action, if said policy outlines the deleting and confidentiality of data. This means the policy would either have to be updated or the change not be implemented. For stakeholders, investments may have been made under the company's past data protection practices. Changing this practice may both upset stakeholders or again be grounds for legal action if written in contracts. For the scenarios above, access to the current user policies and stakeholder contracts are necessary to make an informed decision.

The ACM Code of Ethics and Professional Conduct lays out relevant procedures to the above change. For example “Articulate, apply, and support policies that reflect the principles of the Code”, “Professional Leadership Principles”, and “Respect Privacy”. These sections outline different areas such as how to handle sensitive information, responsibilities of those in positions of influence/authority, and the importance of following and writing clear policies. These ideas would be important to share at following meetings as these concepts directly apply to the changes proposed. In addition it also outlines responsibilities for the individual involved in this conundrum.

This would be my course of action given the situation. First, no decision/implementation will be made until company wide discussion and policy updates. This would require asking the CEO/Managers for an additional meeting before development. In the meeting current standards relating Ethics and conduct will be given as well as the companies past and current policies regarding the change. In the best case scenario the company agrees that the proposed change would be in violation of ethics and data practices. In the other case, changes to the user policy and company policies have to be made. This will make it clear to both users and stakeholders how data is being used by the company. While I might disagree with the practices, clear articulation of how data will be used lets both stakeholders and users make informed decisions on whether or not to continue with the company. If changes are not documented and are hidden from users/stakeholders then the decision would fall on me to cut ties or continue with the company on my own ethical grounds. I joined the company under the goal of “Creating a simple, useful service in exchange for a modest fee”, because of this I believe it would be reasonable to leave the company.