Analyzing the Ethics of Selling Customer Data

There are a lot of questions relating to the ethics of selling customer data, and certainly there aren't (easily) correct answers to all of them since conversations about them are happening all the time today. But there are a few major ones that come to mind, and pertain to this situation in particular, which I'd like to address throughout this analysis:

- Who is impacted when the bundled location data is sold?
    - Who benefits, and in what ways?
    - Who suffers potential or actual consequences, in what ways and to what severity?
- What makes this a difficult decision in the first place?
- What happens if "the right decision" causes me to lose my position at Beerz?

Before I try to answer these questions as a developer, I'd want to talk with the CTO, who seemed to also be concerned about the comments from the CEO. I'd like to see if she has any pieces of advice, since she both has a ton of experience in the field as well as a better understanding of the executive side of the company. I would also like to know how much detail is held within the "anonymized" data to be sold, since specific enough information might allow an attacker to identify specific individuals even through the anonymity. Finally, I'd like to know what my terms of employment are with the company, as it seems that this request goes against my original understanding of the job demands. If I'm employed at will, worse comes to worse, I'll be free to refuse to do something I deem unethical without being worried about breaching an employment agreement.

If I were in this situation, I would refuse to sell any of the data, and I would continue implementing methods to securely dispose of user data once it is no longer needed. As a justification, I think point 1.6 from the ACM Code of Ethics applies to this scenario perfectly:

> Computing professionals should only use personal information for legitimate ends and **without violating the rights of individuals and groups**. This 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**.
>
> ...
>
> **Only the minimum amount of personal information necessary should be collected in a system.** The retention and disposal periods for that information should be clearly defined, enforced, and communicated to data subjects. **Personal information gathered for a specific purpose should not be used for other purposes without the person's consent.**

By selling user data, even in anonymized bundles, Beerz is using personal information for a purpose not previously agreed to by the user. Users are potentially at risk of having their privacy rights violated if the data can be traced back to them somehow, and at the very least selling the data to another company grants that company access to a user's data that was not authorized by that user. This solidly rules out the colleague's suggestion that we pull old data from logged GET requests, since the users making those requests had not agreed to this use of their data. I would also look into the feasibility of purging the API logs so that user data is not inadvertently stored for longer than specified.

It's quite possible that refusing the demands of the CEO could lead to my termination. However, I believe that the CTO should be on my side here because of point 3.1 of the ACM Code of Ethics:

> People—including users, customers, colleagues, and others affected directly or indirectly—should always be the central concern in computing. **The public good should always be an explicit consideration when evaluating tasks** associated with research, requirements analysis, design, implementation, testing, validation, deployment, maintenance, retirement, and disposal. Computing professionals should keep this focus no matter which methodologies or techniques they use in their practice.

As a computing professional in a leadership role, the CTO is tasked with ensuring that Beerz's software is used for the public good, especially in regards to disposal of data. I believe that if it became public knowledge that Beerz sold user data, individuals would be much less inclined to use the app, which is a good sign that selling user data is not in the best interest of the public. In the short term, Beerz is the only group that benefits from the selling of data, and that might not even remain true in the future. And frankly, if the CTO does not side with me on this point, unless they have a convincing argument otherwise, I think it would be for the best that I no longer work for someone who lied to me about the foundational principles of the company.

I do understand that the primary goal of the CEO is to increase the company's profits so that the company can continue to grow. However, this goal should not be immune to questions about the ethics of the methods used to grow the company, and I think that this approach is ethically questionable. And in a case like this where the CTO should have an ethical objection against a request from the CEO, I think it should be a discussion held amongst the executives and/or board members of the company. If they come back with a decision to go forward with this misuse of user data, I would then make the decision to refuse the work on my own ethical grounds, but I believe, perhaps naively, that the CTO would have enough influence to prevent such a scenario from occurring.