Nicholas Vlahos-Sten

Jeff Ondich

Computer Security

13 October 2025

Ethical Analysis of a Security-Related Scenario

I am picking scenario 2.

A: Identify the main ethical question faced by YOU

Your boss is enthusiastically considering a way to monetize user data in a way that goes against your values, your company's values, and probably violates the user agreement your customers signed. I suspect the terms and conditions make no mention that the users' anonymized data would be sold, because at the time they were written Beerz was committed to protecting privacy. No doubt your company violating a past user-end agreement is unethical and potentially illegal, but if you speak up against this monetization plan you risk losing your job, which you like and need to pay your bills. Admittedly, if you tell your boss you don't approve of their plan, they likely won't fire you but they also likely won't listen to you, which puts you in the undesirable position of "do I work for a company doing unethical things, or do I quit and lose my source of income?" If you don't quit, you could try to change the company from the inside or at least curb some of the worst impulses of your boss. Is that good, or are you promoting bad ethics by contributing to the company in the first place?

Even if you disregard the plan to go back and find and sell the data your company was supposed to have deleted, your plan of keeping users' data for a week to add this other feature could be the start of an ethical slippery slope. I think there are ways to implement your plan ethically, so long as you tell your users that you are going to start keeping their data for a week for this purpose (and by tell I mean they should have to read it and opt in not just opt people in automatically and send out a random email declaring the change that only 10% of them will read) and you allow users to opt out of the data collection while still allowing them to access the app's features.

B: For each stakeholder, list their relevant rights

The users of Beerz are the most obvious stakeholders. They deserve the right to privacy. Yes, they can say that they don't care about their privacy, it's their right to give away their data, but they have to be given the option to state their preferences. It goes against their rights to take their data and sell something that isn't ours without giving them input. They also have the right to honest business dealings, and to have confidence that any legal agreement they enter into agreement with will be respected. I know most agreements are designed by companies to protect companies by saying stuff like "hey by using our product you agree you can't sue us" (looking at you, Disney, for when you told the man whose wife died at a Disneyland restaurant after being served food she was allergic to that he couldn't sue because he agreed to mandatory arbitration when signing up for a Disney Plus trial years before), contracts are two way streets. If a company says in a legally binding document that they won't do something, and does it anyway, well, that's illegal.

For you and the CTO, while the right to work and the right to happiness are not legal rights, I believe they're human rights that everyone is entitled to. Here, they are in conflict, as you might not be able to work at this company anymore without increased unhappiness, knowing that you're doing something unethical.

For the boss, they have the right to create a company and sell a product but they don't have the right to sell things other people own, which is what the boss is proposing to do.

C: List any missing info

I'm curious how we're planning to protect the privacy of the user data, in both your and the boss' suggestions. I know you plan to scrub the data after a week, but during that week, is it encrypted, where is it stored, how is it anonymised, I just want to make sure nobody else can steal it. Given that we can access the old, supposedly deleted data, I'd say Beerz 1.0 did a bad job at protecting user privacy. So maybe we can up our security measures. And speaking of the old data, can we delete these old urls, and are they at risk of being hacked into and leaked? Does the GET request solely contain location info, or is there user data linked to said location info? Can anyone access these old urls or do they need developer access to your software? This feels like a data breach waiting to happen.

D: Describe your possible actions

I mean, one option is you could do nothing and let your boss implement the plan. That would guarantee that you keep your good job, but obviously your inaction is letting

something unethical happen and it goes against the company ethos you claim to love. There is a world in which you agree with the boss' plan but add extra security measures to prevent a data breach where the sold anonymous info becomes not anonymous.You could also, quite lamely I might add, admit your past security flaws to your userbase and sheepishly add "hey can you consent to us selling your past data, the stuff you thought we didn't have, you can say no if you do we'll delete it for real this time pinkie promise."

You could talk to the boss to try and convince them to stand down, and you could use a variety of tactics to achieve this result, perhaps playing on their sense of morality, convincing them the data selling plan isn't worth the risk of a scandal or strongmaning them by threatening to quit alongside the CTO if the plan is implemented. You could leak the plan to the public to inform them. You could circumvent the boss by convincing the shareholders or investors this is a bad idea, though I'd rate the probability of that as very low given those types of people tend to be even more money obsessed.

E: Discuss whether the ACM Code of Conduct offers any advice

Here's a few quotes from the ACM to justify my claims. First of all, yeah it's unethical to sell users' data without their consent, and extra unethical to bundle them together without care for privacy features:

"Personal information gathered for a specific purpose should not be used for other purposes without the person's consent. Merged data collections can compromise privacy features present in the original collections. Therefore, computing professionals should take special care for privacy when merging data collections."

Also you ought to be honest and trustworthy. Your company is already lying to its consumers by saying that their data is scrubbed after every session and then not deleting the old urls with their data. But since no harm has been done yet, your company has a chance to make things by deleting the old data and not implementing the data selling plan.

“A computing professional should be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties. Making deliberately false or misleading claims, fabricating or falsifying data, offering or accepting bribes, and other dishonest conduct are violations of the Code.”

And here’s a quote to foreshadow (and justify) my recommendation:

“A computing professional has an additional obligation to report any signs of system risks that might result in harm. If leaders do not act to curtail or mitigate such risks, it may be necessary to "blow the whistle" to reduce potential harm.”

F: Describe and justify your recommended action

My recommended action: I think you should first strategize with the CTO and confront the boss together. Since you haven’t implemented their plan yet, you still have a chance here to nip the problem in the bud without much hassle. The boss may be a well-intentioned dumbass who just sees dollar signs and does not realize that selling other people’s data without their consent is unethical. Maybe explaining to the boss why this plan is so unethical would get them to stop it. Yes, you run the risk of getting yourself fired, but if the boss is so power-hungry that even suggesting they might be

wrong is cause for termination, maybe this company is incapable of fulfilling its aspirational mission and you'd be happier finding a better place to work.

If the boss is unconvinced, perhaps remind them of said company mission, and argue that this action could lose customers who may have bought subscriptions because they believe in privacy. So yeah, not a guaranteed money maker, boss. If you can, perhaps go around the office and get your coworkers to sign a petition agreeing with your stance. Showing this to the boss might convince them that the data selling is not worth a potential internal rebellion. This petition will also help with the backup plan.

If you successfully convince the boss, the next step is figuring out how to permanently delete those old urls containing the "deleted" user data, ASAP. That is a PR disaster data breach waiting to happen.

If you don't successfully convince the boss, I'd recommend anonymously blowing the whistle on what they're doing, and telling Beerz users that the data they thought had been deleted was actually not deleted and matter of fact is being sold without their consent. If part of Beerz' appeal was its privacy promises, its userbase might get real angry about this, boycott, and make it more cost-effective for the boss to scrap the data selling plan. Here's where the petition comes in. If most of the office is angry about the plan, you are much less obviously the whistleblower. With enough plausible deniability to hide behind, you might even keep your job.