

# The Bargain We're Making with Our Privacy, and Our Planet

By: David Alia, Amielee Omboy, Zaijan Sabañico



We live in a world full of trade-offs. We love the convenience of fast, instant communication and endless knowledge—but every download, every scroll, feels like a transaction. And as citizens, we are constantly asked to choose: Do you want *Security* from threats, or do you want *Privacy*, when no one's looking over your shoulder? And lately, we realize that both of those things are crushing our Environmental Responsibility. We can't keep sacrificing our planet just to keep our data flowing.

We've been tricked into thinking we can only pick two—or perhaps just one. This is the great ethical failure of our time. It hatches, creates, and carves anxiety into ourselves, making us feel vulnerable. This constant, exhausting tension forces us to

make adjustments every single day. Logging into an app means trading our own data for service, and buying a cheap device means accepting a mass environmental footprint later. We've become accustomed to accepting these short-sighted failures as inevitable, yet they are nothing more than poor choices rooted in a profound crisis of foresight.

But philosophy recalls that decisions are not necessarily ones of sacrifice; sometimes they are ones of harmony. The wisdom of Aristotle is to seek the mean, and not the extremes. Drowning in surveillance in the name of security is not what we require, nor giving up on all technology for the sake of the earth. The middle way is achievable if we behave with moderation. Kant asks us to recall: *people are not commodities*. Our privacy should never be bought and sold, and our earth should never be discarded. But utilitarianism also pushes us ahead to the future to ask if our actions produce the greatest good for ourselves, of course, but also for those following after us, who will inherit our technology and our atmosphere.

Our current practices fail all three tests—they are rooted in *imbalance*. We reject Aristotle's means by demanding such extremes: companies engage in the excess of hoarding data, failing to see data minimization, which would simultaneously increase privacy and reduce the security burden. This excessive collection of personal information—our habits, our location, our beliefs—is the clearest violation of moral laws. Treating a user's digital identity as a commodity to be mined, bought, or *sold* reduces that individual to a mere means to a corporate end, where it strips away their dignity in the pursuit of profit.

Let us open our eyes and see what we are dealing with. We seek information from them, but we are also giving them our information. Our security risk is high as we are being too open with giving out our information. These companies are risking the data or their users by having little to no security in their program to protect the user's data while providing what the user seeks. But we can't only blame the companies that made the program, as we, too, are to blame. We freely roam around but are not aware of the danger they might come across, how their data will be collected, transferred, or shared.

Hence, we should not only be responsible for what we are doing but also be active in what's happening around us. We can't just keep on looking for what we want when we don't even know what risk we are taking. To protect the company's reputation and the users' data, know what you are doing, be secure, and be prepared. Risking something for another lets you be vulnerable to things that are lurking on the web. *Just because something has security doesn't always 100% guarantee you safety.* There are a lot of cases about their data being leaked, shared, taken, etc., and we can't blame them for doing what they want to do with our data, as we openly let them have it, give them our information by neglecting our safety for their needs.