1. AI Hiring Algorithmic Bias

Researchers at Stanford conducted a hiring study earlier this year to investigate the algorithms used to screen job applicants. Over 90% of U.S. employers use the same vendors to conduct screenings, so the researchers decided to test whether the AI hiring tools used by these vendors showed evidence of discrimination and/or bottlenecks in job opportunities for certain demographics. For the study, they followed 3.4 million real job applicants who submitted 4 million applications to 156 employers across 11 market sectors and evaluated the effect of algorithmic monoculture on their job opportunities.

The study had several key findings. First, 25.87% of applications submitted by Black applicants were adversely impacted by their race. Similarly, 14.74% of applications submitted by Asian applicants were adversely impacted. Overall, they concluded that there was significant evidence to suggest that these AI hiring tools did, in fact, yield racial bias and lead to systemic rejection.

We thought this was a clear example of an unethical practice, as it is discrimination embedded into technological systems. We're extremely disappointed in the findings, but even more disappointed by the fact that no one in the Stanford study got to review the algorithm itself. This means no meaningful change can be made because no one has actually investigated the algorithm's code.

The fault in this example falls pretty explicitly on the product, but we would argue that no product is engineer-independent, and thus there is an onus of responsibility on the engineers as well. The software/AI algorithm is ultimately unethical, but it wasn't intended to be made unethically, so the blame on the engineers is alleviated a bit. However, because no engineer bothered to screen for this beforehand or even investigate this fairly straightforward concern that could arise with a tool like a resume screener, the engineers are to blame as well.

2. Meta Lawsuit Involving Data Selling

Earlier this October, Meta, the company behind some of the biggest social media platforms on the planet, including Facebook, Instagram, and WhatsApp, was fined $25 billion following a trial in New Mexico where it was found guilty of lying about its data practices. The judge explained that "The lies extend beyond Facebook's data practices as well" and that they were "at the heart of Facebook's core business practices". In this specific lawsuit, the firm was alleged to be responsible for willful law violations and misrepresentations to the public that spanned more than 11 years, from 2010 to 2021. The jury found that Meta violated New Mexico's state laws over 40 million times and that all 2 million people in the state were affected by its misuse of data.

What disturbs us most about this situation is that data privacy violations, and more specifically, data mishandling, are things that Meta has been found guilty of many times throughout its existence. Earlier this year, it settled for $18 billion with California over a child safety lawsuit. This fine followed a $5 billion fine that was levied by the U.S. Federal Trade Commission in 2019 after the company was found guilty of unethical data privacy practices. There was also the Cambridge Analytica scandal in 2016, where Meta was found to have utilized the data of millions of Facebook users and sold it to Cambridge Analytica to be used for political consulting.

Overall, this is a clear case of unethical practices by the engineers. While the concept of social media apps or products such as Instagram or Facebook isn't inherently unethical, engineers at Meta have clearly been caught time and time again mishandling the data they collect through their software and using it maliciously. We believe that despite these being optional apps to use, when people decide to trust your app and put their data into it, the company has a moral responsibility to treat the users' data safely, which hasn't been the case for Meta throughout its existence.

3. Software Engineering Roles at Palantir

For our last example, we decided to discuss the ethical implications of working at a defense company as a Software Engineer in 2026. The company we chose to focus this discussion on is Palantir Technologies, as it is an extremely well-known data integration and defense company that best highlights the ethical dilemma we want to discuss.

The ethical dichotomy we want to highlight stems from the appeal that Palantir has for Software Engineers and the national and geopolitical influence of the software it makes. On the one hand, Palantir Technologies is notorious for paying New Grad Software Engineers very well. Levels.fyi reports that New Grads at Palantir can make upwards of $230,000 in total compensation, a number that a majority of New Grads in the tech field are enticed by, as it outpays over 95% of companies with similar roles. At the same time, Palantir also received a $30 million grant from Immigration and Customs Enforcement (ICE) to build surveillance platforms across the United States. Moreover, it is also a huge contractor for the Department of War, helping make software that has been used in weaponry. Overall, we find that the practical uses of Palantir's software create, at the very least, ethical ambiguity for those who work there as well.

Obviously, this is a very multifaceted topic, and it's naive to assume that a person is an "unethical" person just because of a perfectly legal role they work in. The financial independence that a Palantir role could help someone achieve is unique to each person, as each person's financial situation could be affected differently by the role. More than that, the position could genuinely be something the engineer is fascinated by. Finally, an argument can be made that defense companies do nothing but make our cities, states, and country safer, and thus shouldn't be viewed so negatively.

There isn’t really a clear answer as to who the “blame” falls on for this. We believe that if there is a mass surveillance product that a company develops for a country, like ImmigrationOS, the software itself is unethical. However, it is also true that the engineers who built such a surveillance project are equally responsible, if not more responsible, for how unethical the situation is. Ultimately, this is not a one-dimensional conversation and is a heavily debated ethical question among Software Engineering communities.