To: aiframework
Subject: Ai Framework Recommendations
Date: Monday, April 4, 2022 10:39:24 AM

Team,

After participating in the multi-day workshop over slack and zoom, my overarching concern about the framework is the potential to confuse AI security with AI FAT. While FAT and ethics are the most important issues facing AI, there are also actual security issues dealing with model stealing (extraction), intentionally causing model drift, model evasion, and so on.

I fear that trying to tackle both security and FAT in one document may be detrimental to both. In the AI workshop we didn't seem to touch on many of the security issues like "how do we stop model extraction" or "how do we guide government and business in dealing with model evasion". I appreciate the efforts to tackle the hard problems of FAT, but we also need guidance on dealing with the technical security issues facing AI.

Please feel free to contact me if there are any discussions along the lines of security issues like the ones I've mentioned. I am eager to discuss these security concerns.

Grant Baumbach