**HLT – AI**

Responsible AI is the practice of designing, developing, and deploying AI with good intention to empower employees and businesses, and fairly impact customers and society—allowing companies to engender trust with confidence.

Responsible AI can be built into AI to ensure that the algorithms and underlying data are unbiased and show true representation as much as possible. To build trust among employees and customers, developing AI that is transparent across all processes and functions. Furthermore, empowering individuals using AI to raise doubts or concerns regarding the AI system and being able to manage governing that technology without stifling innovation.

To employ a security and privacy-first approach to ensure sensitive and personal data is never used in an unethical manner. By creating an ethical underpinning for AI, it will mitigate risk and establish systems that benefit the user and customers and society at large. Responsible AI is the right thing to do. It helps ensure that any AI system will be efficient, comply with laws and regulations, operate based on ethical standards and prevent potential for reputational and financial damage down the road.

However, there have been instances where AI has failed. Using AI to streamline talent acquisition is common in this day and age. However, it hasn’t always been the case. Amazon had been building software that would automate the process of reviewing job applicants’ resumes with the intention of finding the top 5 talents since 2014. It was later discovered in 2015, their AI-powered recruiting tool was hiring for technical roles in a way that was not gender-neutral. It turns out Amazon had trained their machine learning algorithms on resumes that had been submitted to the company over a 10-year period. The majority of resumes came from men, since this is what was most common in technical roles, and the algorithms learned this pattern and determined women are not good suitors for technical roles.

Another example of when AI had failed and been used maliciously. Facial recognition is very common in 2022, but it may not be as secure as we initially thought. Researchers have been able to find instances in which facial recognition has been fooled using a 3D-printed mask that depicts the face of the face used to authenticate the Facial ID system. This caused Apple to provide updates to its users to reassure them that hackers weren’t able to gain access to their devices.