QSS 20: Social Science Issue

Ryan Dudak

Last updated: September 14, 2023

1 Data Privacy and Generative AI

One social science issue that I care about is protecting sensitive data with regard to the use of generative AI. Companies are jumping at the opportunity to incorporate generative AI into their business processes, but they also need to make sure their customers' sensitive data is protected. One report states that 46% of senior executives surveyed suspect their colleagues of providing snesitive data to ChatGPT (1). Many large language models retain prompt data that is sent for training and validation purposes, including any sensitive data such as PPI, PHI, and financial information. CIOs and other stakeholders wishing to use this technology to personalize interactions must ensure this data isn't viewed or stored by LLM providers.

I believe data privacy in general is an extremely important issue, as people need to be able to feel that they can trust companies with their data. On the other hand, customers are demanding more from companies in the form of more personalized experiences. Generative AI has the potential to deliver on these more personalized experiences, but it cannot come at the cost of data privacy and security. Comapnies and individuals must make an effort to educate themselves on responsible and ethical use of generative AI and other data-dependent technologies.

References

[1] A. Divatia. Council post: How companies can use generative ai and maintain data privacy, Jun 2023.

Figure 1: Highly regulated industries like financial services and healthcare handle tons of sensitive data.