DAMA DAY

WARSAW

18 SEPTEMBER 2025

AI and Data Privacy: We need Both

Frank Kadwell, PhD
763.442.5620
Frank Kadwell Email

Agenda

Data Security and Data Privacy

AI, Algorithms, and Ethics

AI models and their effect on data privacy and security

How do we move forward

Data Security and Privacy

Data Security and Data Privacy are DIFFERENT

Data Security is how we keep the data safe

Data Privacy is about keeping data private and having control of our data

Ethical handling of data privacy and security with AI

Qualities of AI

Predictive modeling, where the model has a lot of feedback

Sports like football, baseball

Continuous feedback and model tweaking

Overall model improvement

Drawbacks of AI

Bias within the models

Keeping models secret and not knowing the DATA behind the models

Lack of data privacy and security

Examples of AI and Algorithm Bias

AI being used in the hiring and firing of employees

AI being proposed in law enforcement (In the United States)

Housing in the United States

LACK FEEDBACK and TRANSPARENCY

The needs of AI Models

AI models need DATA

The need for data creates friction between data privacy and security and the want or need to have large amounts of data

AI models will make predictions, whether data is well sampled or not

how do we protect privacy AND take advantage of what AI has to offer

Data Quality

Continue data quality initiatives even on a large scale

Automate data quality efforts to be able to cleanse large data sets

Metadata efforts and making sure we understand the data in context

Understand the context in which the data is collected

Protect data privacy

Continue to enact regulation that protects the public and their privacy

Laws like GDPR – continue to improve as AI matures

The United States is WAY behind

Personal data includes our likeness. We own our whole selves

Algorithm UNDERSTANDING

Algorithm TRANSPARENCY – Yes algorithms need to be public

Understanding not just what the algorithm does but how it collects the information

Ensure the data the algorithm is using is of the highest quality

Protecting and securing the data that the algorithm is using

Algorithm NEUTRALITY

In the United States, private companies often fund research, this creates bias

At least disclose all funding sources

Take it further and choose funding carefully where possible

Find neutral funding sources – entities that are interested in the research, not the results

Open Source as an Option

Built in transparency

Views of the source code AND the source data sources

In many ways better security

Not for everything but is a good option

Conclusion

AI is here to stay

We can secure data AND protect our privacy, and we must

Transparency over corporate need for secrecy

Better regulation and scale up and out data quality

Questions???