Adoption of AI within regulated industries

Debjani Roy Ryan

My background

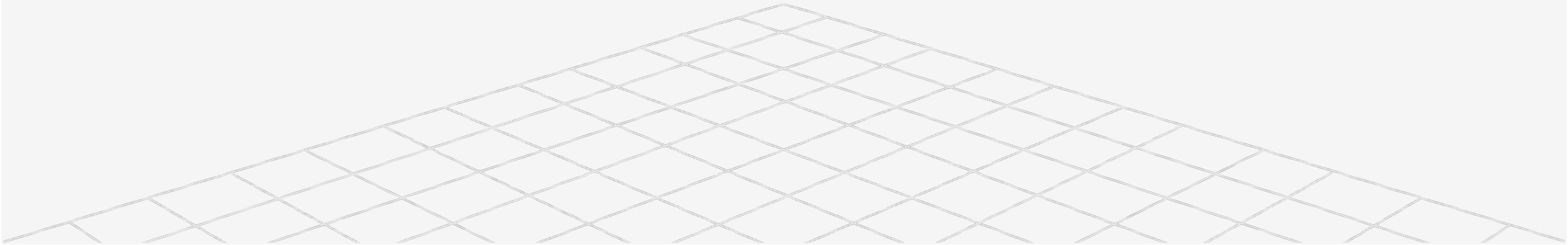
Led engineering for Citibank's corporate banking platform CitiDirect carrying 4 trillion dollars a day

Led data engineering and data science for Barclays – Financial Crime and Surveillance

Led data engineering and data science for Groupon and BT

Led data engineering and data science for a major aviation player

Currently running my own company developing AI Radiology software



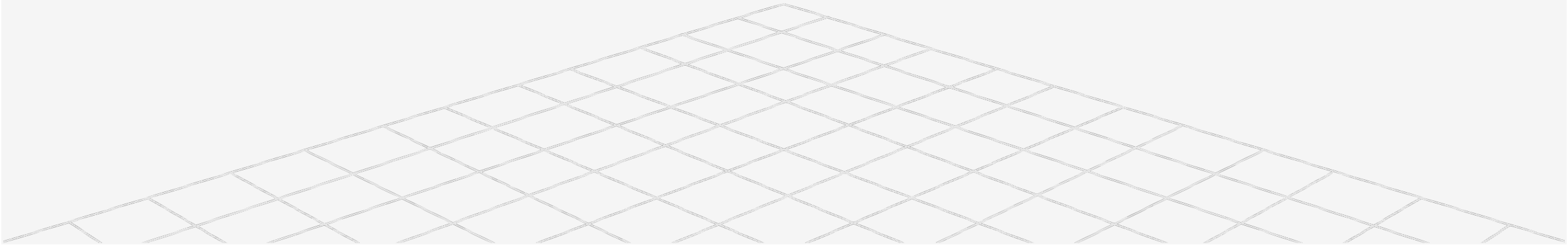
What are regulated industries

Financial services, healthcare , pharma , telecoms are all regulated industries where regulators assess the risk of a deployed model.

Deploying a model in production will involve regulatory submission and liasing with regulators, convincing them of the efficacy of your model

Consider the implications of various laws EUAI Act, UK AI regulation , GDPR when developing a model

Different regulators have different approaches – financial services do not like blackbox models , healthcare accepts blackbox models as long as they are clinically validated with clinical trials



Case study : Major bank

Model to detect financial crime

Ultra-high sensitivity of data with geo political considerations.

Data residency in multiple jurisdictions.

Unbalanced sparse data

Data needs to be tokenised and not masked to develop model. However tokenisation is very expensive in cloud.

Explainable AI – explain the importance and weightings of each feature.

False negatives have high liability – for example a false terror finance suspect.

Detailed regulatory submission

Human in the loop and dual- human/AI running for multiple years.

Consider the financial implication of having a human in the loop in operations and high false positives.

Case study : Be careful about liability

Lawyers don't care about statistics.

Legal challenges have cost implications.

Liability is with institution but in some cases within banks compliance officers may have personal liability

This makes the culture extremely risk averse

Stakeholders may reduce false negatives at the cost of having more false positives.

Demographic data may not be used – only behavioural data

High number of false positives require human in the loop intervention and may reduce efficiency of AI enabled operations

Case study : Healthcare

Model to detect rare diseases

Data residency in multiple jurisdictions.

Data needs to be tokenised and not masked to develop model to take into account demographic features

PII needs to be stripped of data

Extremely unbalanced and sparse data

False negatives have high liability – for example a misdiagnosed cancer patient. Assign higher misclassification costs

Detailed regulatory submission

Human in the loop and dual- human/AI running for multiple years for clinical study

Formal clinical trial design – multiple populations, prospective vs retrospective

Case study : Aviation

Model to dynamically price airline tickets

Data residency in multiple jurisdictions.

PNR data cannot be mingled with passenger data – hence limited use of demographic features

PII needs to be stripped of data

Realtime model with reinforcement learning – has to adapt quickly to market conditions, major events , weather patterns etc

No regulatory submission as it is business sensitive but will not cause harm to passengers

Extremely cost sensitive industry – be mindful of cloud costs

Case study : Telecoms

Model for customer service

Data residency in multiple jurisdictions.

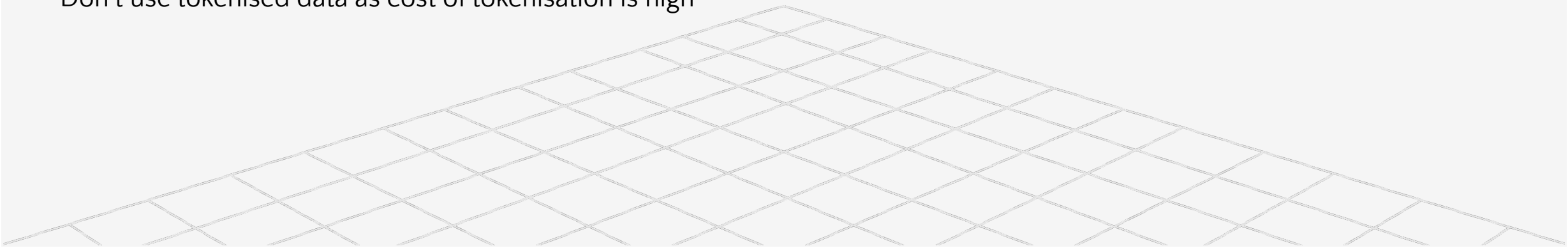
PII needs to be stripped of data

LLM model

Extremely cost sensitive industry – be mindful of cloud costs

Extremely privacy sensitive industry – don’t use PII

Don’t use tokenised data as cost of tokenisation is high



Takeaways

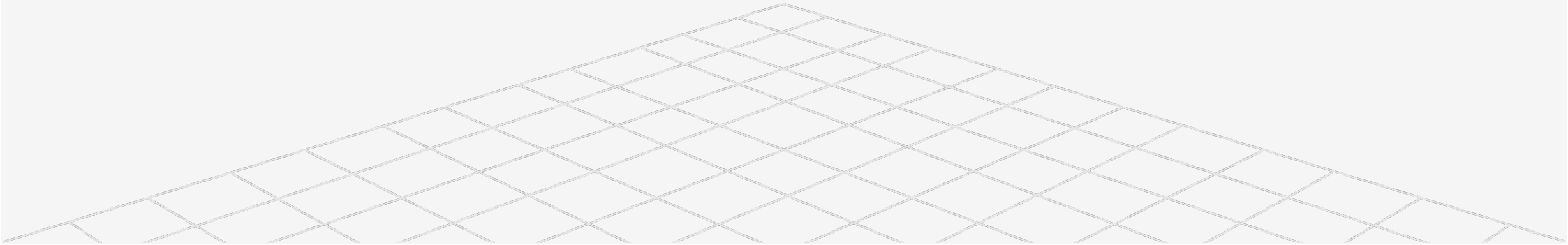
Understand the culture of the industry – cost sensitive, privacy sensitive, security conscious, liability or reputation conscious.

You might have to educate stakeholders on innovation. Regulators for the most part don't understand agile , experimentation although some do have sandboxes

Bring Risk, Compliance, Legal and Finance as part of your team.

Be comfortable with lawyers – they don't do fail-fast in high stakes high risk organisations like systemically important banks.

Be comfortable with finance – if you do not predict cloud costs and model efficiency reliably you may lose your credibility particularly in cashflow sensitive industries.



Thank you