MANAGE AI RISK – ETHICAL DATA & AI – LET'S PLAY.

Karan Dhawal – Data and Transformation Leader - ZS

Phil Finucane – CTO - Pat Inc

Prepared for Data Management Association (DAMA) Wisconsin
https://widama.org/

Image Credit: Texas A&M

EXPECTED TAKE-AWAYS

- Understand guiding principles of ethical AI
- Join in quiz from real world examples to learn about ethical AI
- Question the principles: How might these apply to your organization? What can be added or improved in key ethical AI principles?

REGULATIONS IN AI ARE EVOLVING

> Historically, innovation has routinely outpaced regulations

> In today's digital world, protecting against ethical data usage issues is very important for company reputation and growth

> Worldwide business spending on AI is expected to hit $50 billion this year and $110 billion annually by 2024 – Harvard Education

> "The regulatory bodies are not equipped with the expertise in artificial intelligence to engage in [oversight] without some real focus and investment," -- Joseph Fuller, professor of management practice at Harvard Business School

Artificial Intelligence Risk Management Framework- AI RMF

Artificial Intelligence5 ('the Draft AI Act')

Bill for the Algorithmic Accountability Act of 2022

Blueprint for an AI Bill of Rights
Making Automated Systems Work for the American People

Organization for Economic Co-Operation and Development ('OECD'): AI Principles

International Organization for Standardization ('ISO')
ISO/IEC 23894:2022
Information technology — Artificial Intelligence

Not an exhaustive list

TYPICAL CONCERNS AROUND AI

- Privacy & Surveillance
  - How can my data be used to identify & track me?
  - Can my data be used to train new models and what are the impacts of that on me?
  - Differential privacy
- Discrimination & Bias
  - Are our models fair?
  - How do we prevent human biases from creeping into our models?
  - How do we identify it when we get it wrong?
- Human Judgement / AI for Good
  - What are the types of tasks that we want AI to handle?
  - How do we prevent malicious use of models to create malicious or intentionally deceptive content?
  - Do we want the AI flying our drones or launching our nuclear missiles?

SIX GUIDING PRINCIPLES: "ETHICAL AI"

- Identify AI applications that are too risky to use
- Vet compliance requirements
- Comply to applicable regulations
- Avoid algorithmic discrimination

Accountability

- Enable Oversight on Market Use of AI
- Get AI functionality to general acceptance
- Communicate inaccuracies – AI recall concept
- Opt out of AI systems and fall back to Human

Adoption

Reliability

- Data protection compliant
- Validated for unbiased decisions
- Repeatable comprehensible decisions

- Data Privacy Surveillance
- Data collection conforms to reasonable expectations
- Enhanced protections for sensitive data

Privacy

Explainability

- Harmonize the rules of AI applications
- Communicate rules and decisions by AI
- Notice & Explain perceived economic value to customer

Security

- AI process and infrastructure is secure
- Enhanced protections for AI decision database
- Detect Poisoned training data
- Track denial of AI services

Not an exhaustive list

slido

JOIN
AT **SLIDO.COM** WITH
#1638112

You're a Tourist at the Statue of Liberty. In the museum you opt in to take a picture and provide your name, location and demographic data.

?

Is it be ok to use this data to:

1. Train a facial recognition neural network?
2. Create an AI-powered recommendation platform to generate personalized marketing information?
3. Analyze visitor arrival & departure times to better predict future staffing needs?
4. Package your data with other visitors to create monetizable data products?

You complete an online purchase with a new website and provide your name, address, email, and phone number.

?

Can we use demographic data to:

1. Sell to a data aggregator?
2. Train a model that makes product recommendation to the site's customer?
3. Training models for forecasting market trends.
4. Aggregating customer data to categorize and classify customer segments.

Should the bank be allowed to:

1. Build a model that can predict your future expenses and notify you when you're at risk of dipping into savings?
2. Train models to detect fraudulent activity?
3. Analyze purchase data to predict which stocks to buy or sell?
4. Create a model that detects changes in spending patterns that might indicate significant life changes?

?

Your bank is looking to expand the use of its historical customer transaction data.

?

Is it alright to:

1. Use facial recognition to identify your closest friend to improve cross promotion revenue?
2. Validate the performance of a facial recognition system?
3. Analyze locations in your photos to generate a profile of your vacation preferences?
4. Generate products for consumers without first obtaining permission.

Your cloud-based photo album is leveraged by providers.

We’re building a mortgage approval model.

?

Which data elements would be ok to use?

1. Race / ethnicity / protected group status
2. Home address
3. Income level
4. Credit score

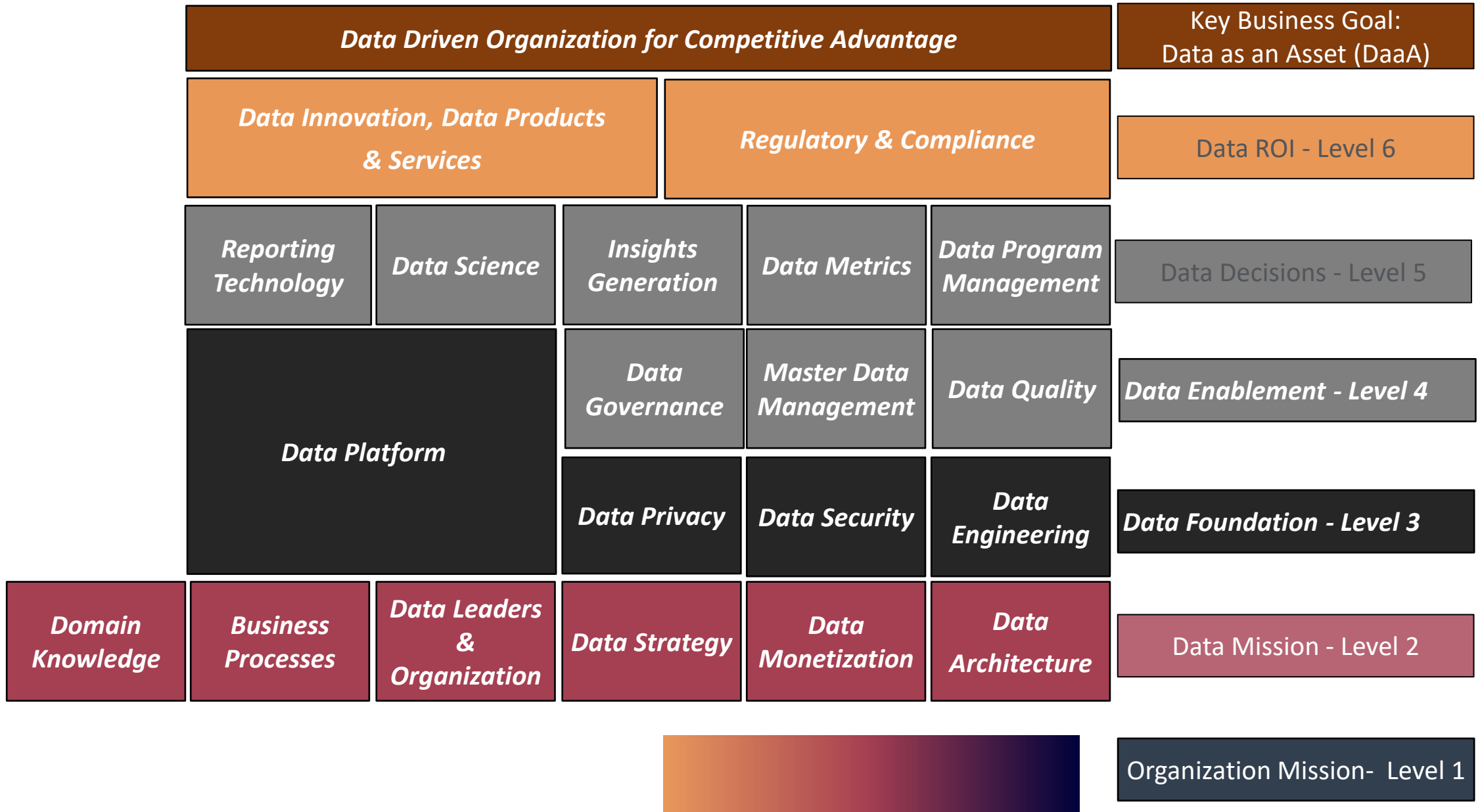
QUESTIONS

WHAT CAN BE ADDED OR IMPROVED IN ETHICAL AI PRINCIPLES?

HOW CAN YOU VALIDATE THAT YOUR MODELS DON’T HAVE BIASED OUTCOMES?

Enterprise Data Management Blocks Framework by Karan (TDAN)

Growth, Productivity, Profitability, Differentiation, Customer Experience and ……



USA DATA PRIVACY LAWS

California	California Consumer Privacy Act of 2018 (CCPA)	In effect
Virginia	Consumer Data Protection Act (CDPA)	In effect
California	California Privacy Rights Act of 2020 (CPRA)	In effect
Colorado	Colorado Privacy Act (CPA)	In effect
Connecticut	Connecticut Act Concerning Personal Data Privacy and Online Monitoring (CTDPA)	In effect
Utah	Consumer Privacy Act (UCPA)	December 31, 2023
Florida	Florida Digital Bill of Rights (FDBR)	July 1, 2024
Oregon	Oregon Consumer Privacy Act (OCPA)	July 1, 2024
Montana	Consumer Data Privacy Act (MCDPA)	October 1, 2024
Iowa	Iowa Consumer Data Protection Act (ICDPA)	January 1, 2025
Texas	Texas Data Privacy and Security Act (TDPSA)	January 1, 2025
Delaware	Delaware Personal Data Privacy Act (DPDPA)	January 1, 2025
Tennessee	Tennessee Information Protection Act (TIPA)	July 1, 2025
Indiana	Consumer Data Protection Act (ICDPA)	January 1, 2026

In Effect
Act Now – Coming Up
Plan – 14+ Months to effect

Reference: Data Guidance