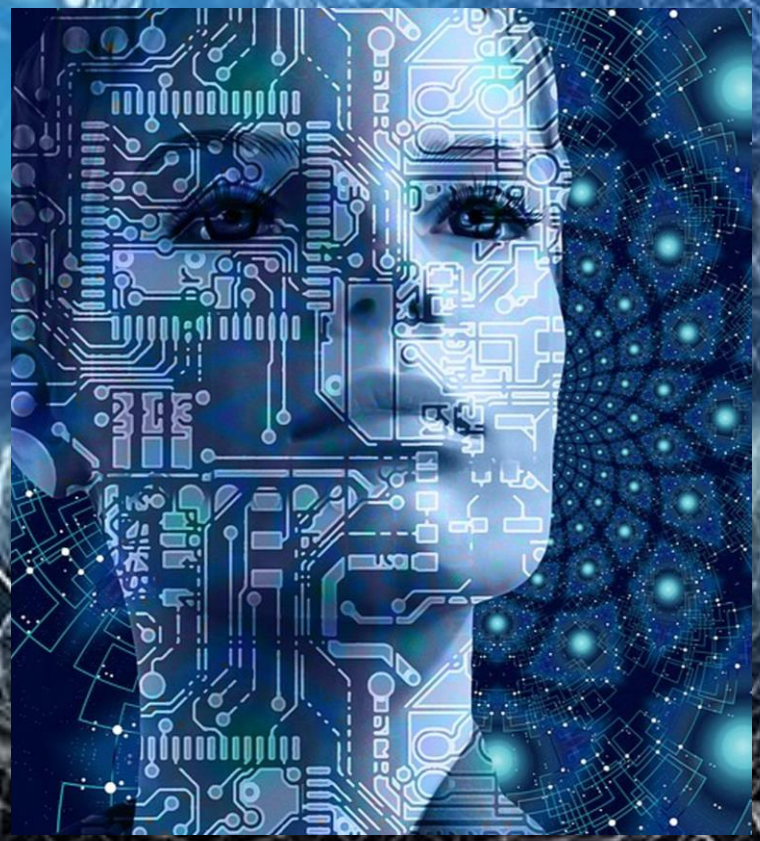
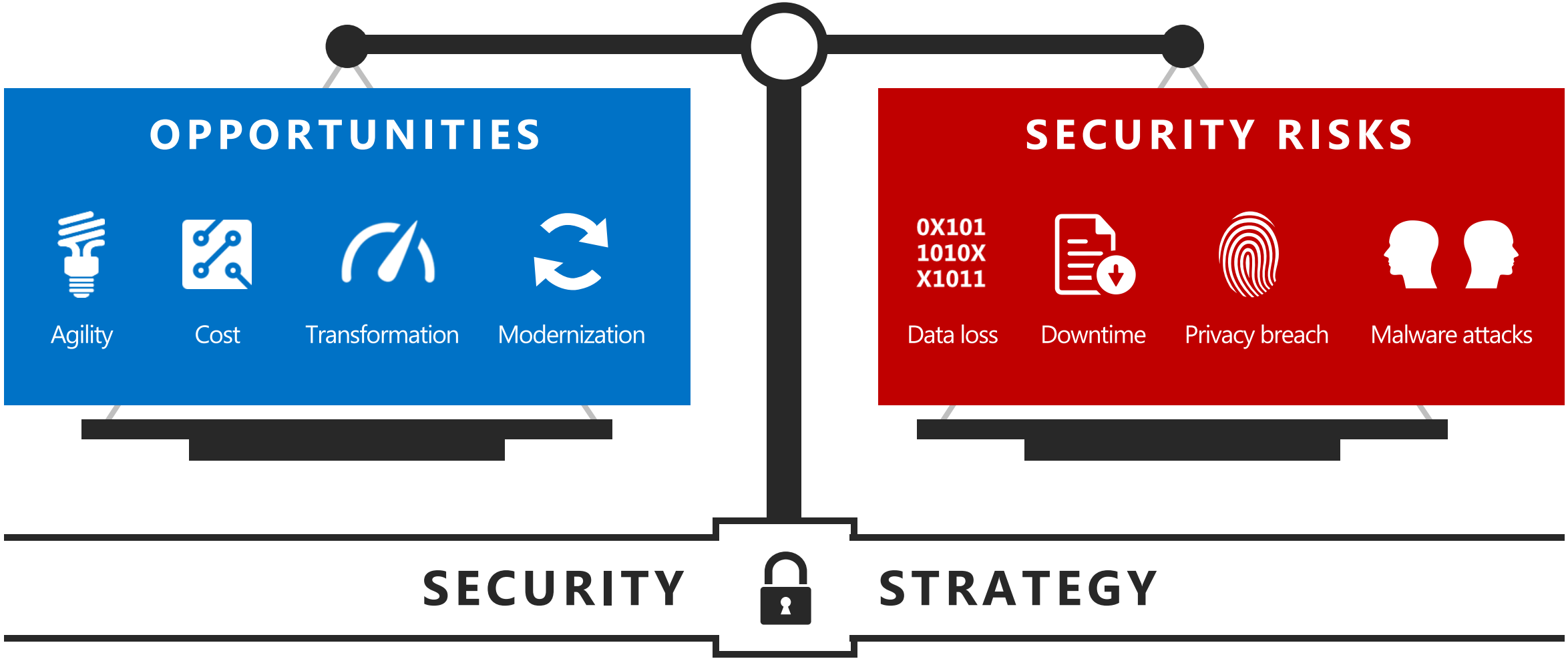
Data Governance
Balancing Data Opportunity With Privacy Protection

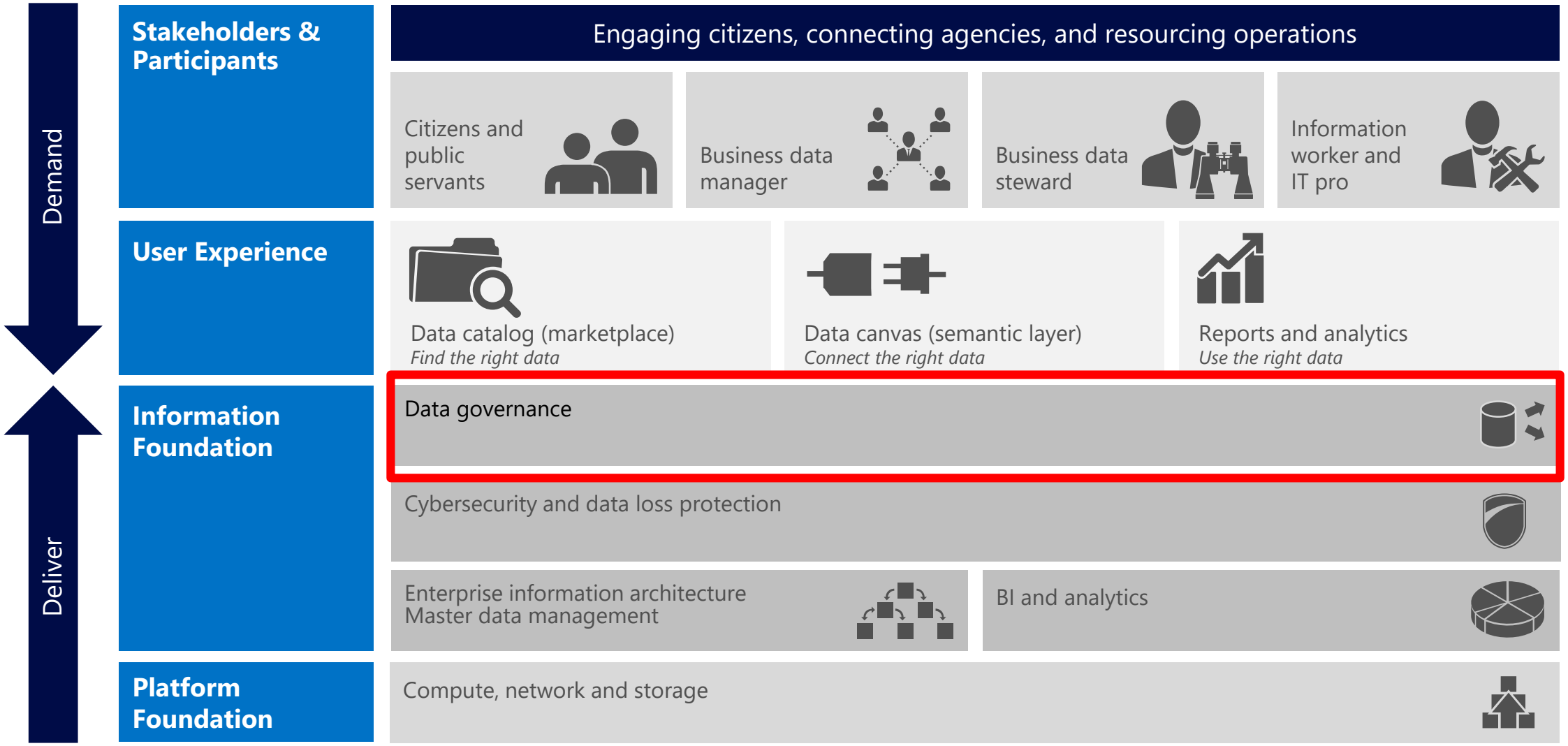


Lesly Goh
Senior Technology Advisor
World Bank Group
Oct 8, 2019

Balance opportunities and risks



Architecture strategy: Technology, Process, People



EU – AI and Data Guidelines

Human agency and oversight — AI should not trample on human autonomy. People should not be manipulated or coerced by AI systems, and humans should be able to intervene or oversee every decision that the software makes.

Technical robustness and safety — AI should be secure and accurate. It shouldn't be easily compromised by external attacks (such as adversarial examples), and it should be reasonably reliable.

Privacy and data governance — Personal data collected by AI systems should be secure and private. It shouldn't be accessible to just anyone, and it shouldn't be easily stolen.

Transparency — Data and algorithms used to create an AI system should be accessible, and the decisions made by the software should be "understood and traced by human beings." In other words, operators should be able to explain the decisions their AI systems make.

Diversity, non-discrimination, and fairness — Services provided by AI should be available to all, regardless of age, gender, race, or other characteristics. Similarly, systems should not be biased along these lines.

Environmental and societal well-being — AI systems should be sustainable (i.e., they should be ecologically responsible) and "enhance positive social change"

Accountability — AI systems should be auditable and covered by existing protections for corporate whistleblowers. Negative impacts of systems should be acknowledged and reported in advance.

Source: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

Monetary Authority of Singapore (MAS) FEAT Principles

Fairness	• Justifiability – use of personal attributes as input factors is justified • Accuracy and Bias – review of data and models for accuracy, relevance and minimize unintentional bias
Ethics	• Use of AI is aligned with firm's ethical standards • AI-driven decisions have same ethical standards as human-driven decisions
Accountability	• AI-driven decisions are approved by an appropriate internal authority • Data subjects are provided with channels to enquire, submit appeals about AI-driven decisions that affect them
Transparency	• Data subjects are provided clear explanations on what data is used to make AI-driven decisions • Use of AI is proactively disclosed to data subjects

Source: https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf

PROPOSED AI GOVERNANCE FRAMEWORK

OBJECTIVES

- Explaining how AI systems work and verifying that they work consistently
- Building in good data accountability practices
- Creating open and transparent communication between stakeholders

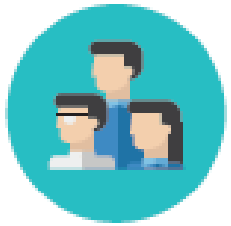
ORGANISATIONAL GOVERNANCE MEASURES

GOVERNANCE

- Putting in place internal corporate governance and oversight processes
- Taking measures to identify and mitigate risks or harm
- Reviewing how and where AI is deployed within the company periodically

OPERATIONS MANAGEMENT AND SYSTEMS DESIGN

- Having good practices in managing data
- Ensuring AI performs consistently
- Understanding what data was used to make algorithmic decisions
- Training and maintenance of AI models



CONSUMER RELATIONSHIP MANAGEMENT

TRANSPARENCY

- Policy for disclosure
- Policy for explanation

COMMUNICATION

- Establishing a feedback channel
- Reviewing decisions made by AI

INTERACTION

- Reviewing human-machine interactions for user friendliness
- Providing an option to opt-out

DECISION MAKING AND RISK ASSESSMENT

- Determining the appropriate decision-making approach to maximise benefits and minimise risk of harm.
- **"Human-in-the-loop"** involves a human who relies on intelligent systems but ultimately makes the final decision
- **"Human-over-the-loop"** involves a human who has made a choice but relies on intelligent systems to suggest options to perform an action
- **"Human-out-of-the-loop"** involves automated decisions by intelligent systems based only on a pre-determined set of scenarios

Source: Singapore PDPC
https://www.pdpc.gov.sg/Resources/Discussion-Paper-on-AI-and-Personal-Data

TRUSTED DATA SHARING FRAMEWORK

PART 1: Data Sharing Strategy

1.1 Establish Data Sharing Potential and Value of Own Data

1.2 Understand Potential Data Sharing Models

1.3 Consider Engaging Data Service Provider to Facilitate Data Sharing

PART 2: Legal and Regulatory Considerations

2.1 Determine if Data Can Be Shared

2.2 Establish Data Sharing Agreement

PART 3: Technical and Organisation Considerations

3.1 Prepare Data for Data Sharing

3.2 Understand Technical Considerations for Data Sharing

PART 4: Operationalising Data Sharing

4.1 Ensure Transparency and Accountability

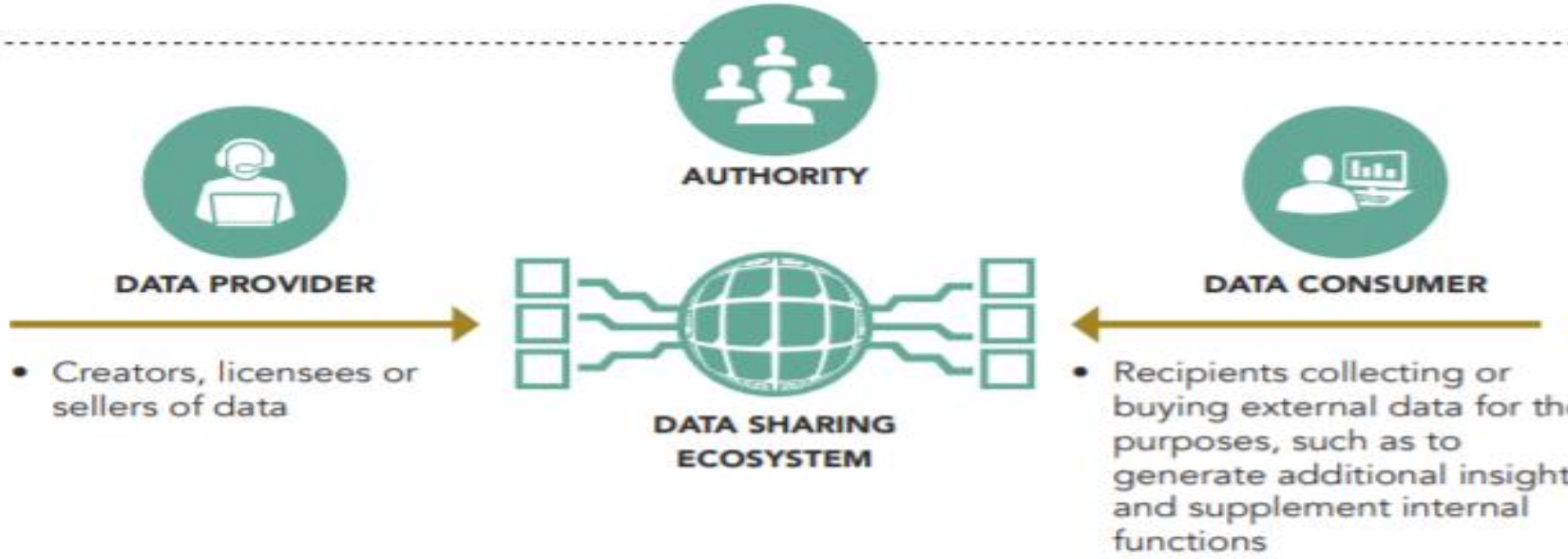
4.2 Monitor Ongoing Legal and Regulatory Obligations

4.3 Use of Data for Secondary Purpose

4.4 Understand Considerations for Retention and Disposal of Data

Source: Singapore
https://www2.imda.gov.sg/programme-listing/ai-data-innovation

- An institution or organisation empowered to operate a supervisory function related to the ecosystem
- May refer to the regulator (or other governing bodies), or industry bodies with oversight mandates or other practical influence (e.g. industry associations, standards institutes)
- Usually not directly involved in data sharing, but can influence the data sharing activities through legislative reviews, issuance of the guidelines, standards or accreditation schemes



- Creators, licensees or sellers of data

- Recipients collecting or buying external data for their purposes, such as to generate additional insights and supplement internal functions

DATA SERVICE PROVIDERS

- Organisations providing data services supporting the data sharing ecosystem
- Services can include, but not limited to, the following:
  (1) providing technical means (e.g. platform) to facilitate data exchange;
  (2) data preparation, data management and technical/ risk/ governance advisory; and
  (3) acquiring data from providers (may include processing to enhance its value) and supplying data to Data Consumers or marketplaces.

Questions for this Panel

1. How do financial institutions collect, manage, and utilize their clients' data? What are the challenges and opportunities in this area?
2. How should financial intuitions balance financial innovation (how they use the data), while complying with regulatory requirements and acting responsibly towards their clients?
3. How can regulators create an environment that encourages responsible use of data for MSME credit risk management, while ensuring both market stability and a level playing field for banks and the new alternative lenders?
4. Who should own the data? How can borrowers assure the accuracy of alternative data inputs used to evaluate their creditworthiness and transparency of pricing terms?