Artificial Intelligence Governance in Singapore

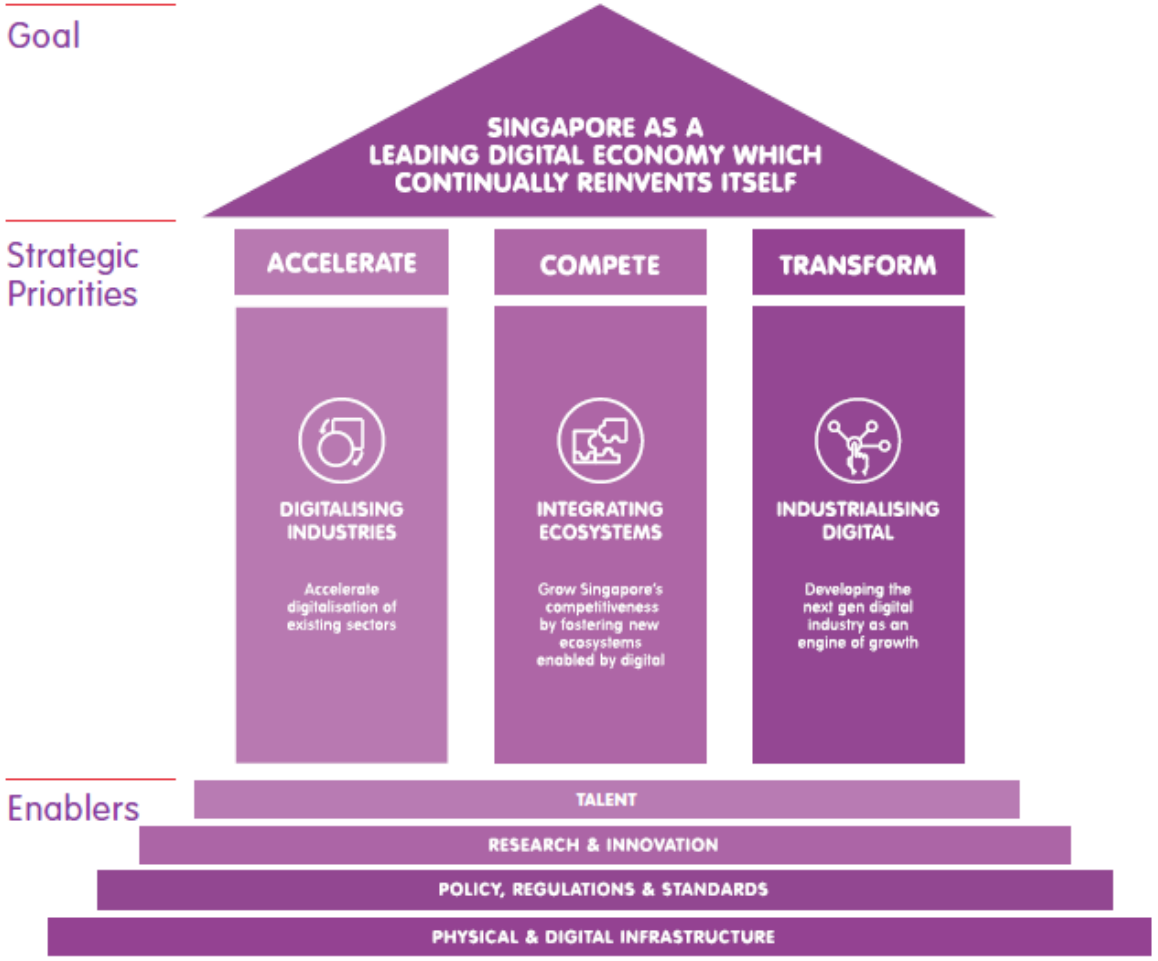
Yeong Zee Kin

Deputy Commissioner, Personal Data Protection Commission

Assistant Chief Executive, Data Innovation & Protection Group

Infocomm Media Development Authority of Singapore

Digital Economy Framework for Action



Use and share personal data innovatively and responsibly → Competitive advantage for businesses

Infusing AI into business operations → Accelerate digital transformation

In 2016, companies invested
US$26B to US$39B
In artificial intelligence

Tech Giants
US$20B to US$30B

STARUPS
US$6B to US$9B

Source: Mckinsey Global Institute, Artificial Intelligence, The Digital Frontier

Need to promote responsible deployment of AI to engender consumer trust & willingness to use AI solutions

Opportunity for Singapore to balance between technology innovation and consumer concerns through enabling regulations

Consumer Empowerment

Public Trust & Confidence

Business Friendliness

Technology Innovation

Image Source: VectorStock.com

Advisory Council on Ethical Use of AI and Data

Why an Advisory Council?

- Provide guidance on complex ethical issues arising from new business models and innovation in AI space
- Barometer of business needs and consumer sentiments to shape Government's plan for sustainable AI ecosystem

Who are Council Members?

- AI technology providers
- Businesses that use AI
- Representatives of societal and consumer interests

How to achieve Council's goals?

- Engagement and dialogue sessions with industry and consumers

What are Council's work products?

- Model AI Governance Framework
- Voluntary industry codes of practice

Discussion paper on responsible AI to trigger public dialogue

Why a Discussion Paper?

- Propose accountability-based framework for responsible development and adoption of AI
- Promote structured discussion on ethical, governance and consumer protection issues
- Promote understanding and trust in AI technologies

Strategic Considerations

PROMOTE

- ✓ DEVELOPMENT & ADOPTION OF AI
- ✓ INNOVATION, COMPETITION & CONSUMER CHOICE
- ✓ CONSISTENCY IN DECISIONS MAKING

Principles of Responsible AI

DECISIONS MADE BY AI SHOULD BE **EXPLAINABLE, TRANSPARENT AND FAIR**

AI SYSTEMS, ROBOTS AND DECISIONS SHOULD BE **HUMAN-CENTRIC**

AI Governance Framework

Proposed Reference 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

Research Programme on Governance of AI & Data Use

Why a Research Programme?

- Build up a body of knowledge of legal, policy and governance issues concerning AI and data use
- Develop a pool of experts knowledgeable in these issues
- Complement existing efforts to strengthen scientific research (AI Singapore) & professional training in AI (Tech Skills Accelerator, TeSA)
- Develop Singapore as a thought leader in AI legal and governance issues

Who hosts this Research Programme?

- SMU School of Law
- In collaboration with local and international partners

What are the deliverables?

- Research and publications
- Local and international workshops, seminars, symposiums, conferences

Interlinked AI governance initiatives to support Singapore's AI development and innovation

Advisory Council on the Ethical Use of AI and Data

Composition

- Industry-led
- Private sector thought leaders
- Consumer advocates

Roles: Advise and support Govt to:

- Identify regulatory, legal, policy, ethical and governance issues in commercial deployment of data-driven technologies
- Provide insights and recommendations on issues that may require policy consideration/ regulatory/legislative intervention
- Develop ethics standards and reference governance frameworks and publish advisory guidelines, practical guidance, and/or codes of practice for the voluntary adoption by the industry
- Providing insight and guidance to the Research Programme

Provide industry & consumer perspectives

Provide regulators' perspectives

Research Programme on Governance of AI and Data Use

Executive Committee
(NRF, AI SG, IMDA, SMU)

Management Team
(SMU)

Discussion paper: AI and Personal Data – Fostering responsible development and deployment of AI

Regulators Roundtable on AI Governance

Composition

- Sector regulators and public agencies

Roles

- Community of Practice for public agencies
- Establish common AI governance principles and framework across sectors
- Co-ordinated, principled and outcome-focused sectoral regulations where necessary

Data Protection Issues in DLT Records (1/3)

- DLT records are typically used transactional records for transfers of value, eg cryptocurrencies, title registry, data accountability & provenance tracking (i.e. RegTech)
  - DLTs are well suited audit trails and transactional records
  - Permissionless DLTs can be accessed or written by anyone
    - But entries in DLTs are encrypted but accessed through an application layer
  - Permissoned DLTs are closed to club members

- Protection obligation – s 24 PDPA; principle of integrity and confidentiality – Art 5(1)(f) GDPR, security of processing – Art 32 GDPR
  - Reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks
  - DLT effective in preventing modification or data loss
  - But poses disclosure risks

Data Protection Issues in DLT Records (2/3)

- Retention limitation – s 25 PDPA; principle of storage limitation – Art 5(1)(e) GDPR
  - Cessation to retain personal data or removal of the means by which it can be associated with individuals when purpose for collection fulfilled and no longer necessary for legal or business purpose
  - Blockchain entries can't be archived or deleted – but what about disposing of the encryption keys?
  - Same issues faced in jurisdictions with right to erasure (Art 17 GDPR)

- Correction – s 22 PDPA; Rectification – Art 16 GDPR
  - Must correction of personal data entail erasure of old records?
  - If no correction is made, organisation to "annotate the personal data … with the correction that was requested but not made"
  - Can this be extended to annotation of outdated records and inserting a pointer to the updated record?

- Anonymisation –
  - Data is no longer personal if recipient is unable to identify the individual
    - From data itself or any other data recipient has access to
    - *cf* anonymisation guidelines (Chapter 3, Selected Topics Guidelines)
  - Assessment not just at DLT record layer but also the application layer (e.g. cryptocurrency wallet)

Data Protection Issues in DLT Records (3/3)

- Transfer limitation – s 26 PDPA; Art 44 GDPR
  - Transfers out of Singapore only to organisations that provide a comparable standard
  - Requirements for transfers: reg 9 PDPR
    - Consent
    - Contract performance
    - Data in transit
    - Publicly available
  - Consent requirements:
    - Summary of extent of transfer and countries
  - DLT records face the same challenges are use of cloud computing

- Potential use of DLT for cross border KYC
  - *Consortium of banks, together with IMDA Singapore, completes proof-of-concept for ASEAN's first industry KYC Blockchain*, OpenGov (28 Oct 2017)
  - KYC records are personal information
  - Can KYC records come within the credit reports exception?
  - Would KYC records come within future "legitimate interest" exception?

Thank You