THE UNIVERSITY OF MELBOURNE

Demystifying AI: Ethics, Law and Regulation

Professor Jeannie Marie Paterson
CAIDE and Melbourne Law School
jeanniep@unimelb.edu.au

AI Harms

- Privacy eroding
- Biased
- Inaccurate
- Not robust — parameter
- Cyber risks — data breach

But human decision makers are also flawed?

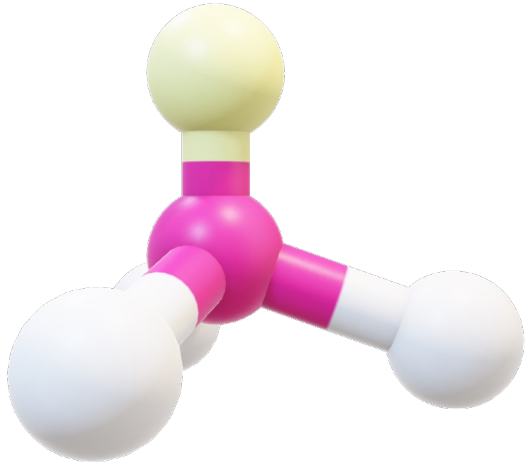
Complications in reviewing AI informed decisions

- Personalisation
- Lack of transparency
- Scale
- Speed

What is the best (legal) response to these concerns?

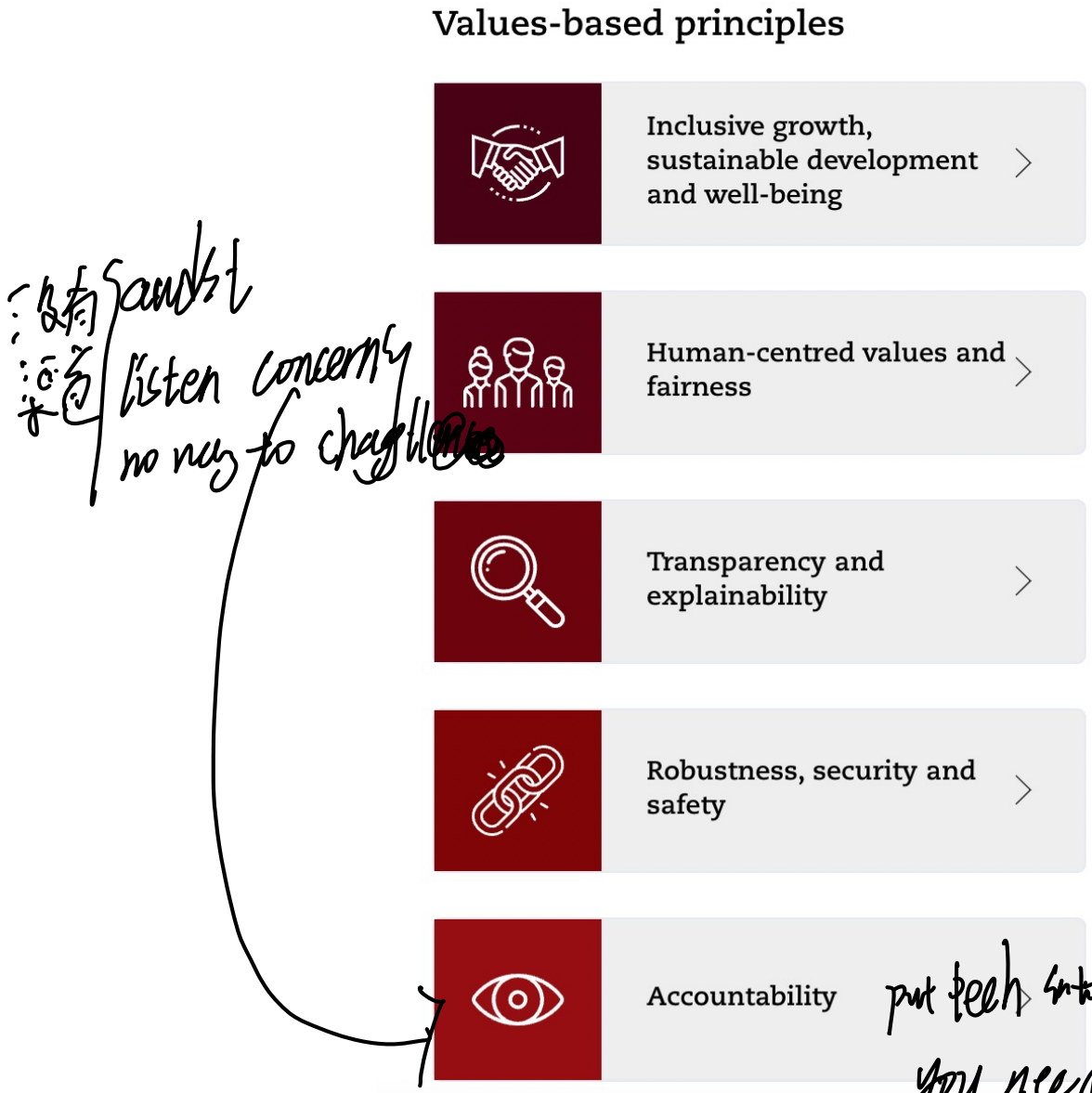
Four models

- Soft law codes eg AI ethical principles
- Data protection law
- General principles
- Laws specifically on uses of AI



1. Principles of AI ethics?

OECD Principles of AI Ethics



internal external

AI Ethics (soft law code)

Weak response, or

Informing general law?

ethical AI is soft law codes

2. Data protection law

Controlling the flow of data

- General Data Protection Regulation (EU) (GDPR)
- Privacy Act 1988 (Cth)

Privacy Act 1988 (Cth)

Privacy Act 1988 (Cth): governs the collection and use of personal information by Australian government agencies; private entities (companies, NGOs etc) with an annual turnover greater than $3 million; and some other entities in limited circumstances'

The rules are expressed in the "Australian Privacy Principles" APPs: https://www.oaic.gov.au/privacy/australian-privacy-principles/

What does the Privacy Act Protect?

The *Privacy Act* regulates the way an individual's personal information is handled.

'Personal information' is any 'information or an opinion about an identified individual, or an individual who is reasonably identifiable: (s 6(1))

OAIC considers that 'personal information' includes 'voice print and facial recognition biometrics (because they collect characteristics that make an individual's voice or face unique)'

https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-personal-information

How do firms justify collecting personal information of personal information?

Australian Privacy Principles – an APP entity

may only solicit and collect personal information that is reasonably necessary for one or more of its functions or activities (APP 3.1 and 3.2)

may only solicit and collect sensitive information if the individual consents to the sensitive information being collected, unless an exception applies (APP 3.3)

that collects personal information about an individual must take reasonable steps to provide notice. (APP 5)

social media 的 bussiness model: 决定他们要不要收集个人信息 → marketing

Sensitive personal information

Sensitive information is personal information that includes information or an opinion about an individual's:

racial or ethnic origin

political opinions or associations

religious or philosophical beliefs

trade union membership or associations

sexual orientation or practices

criminal record

health or genetic information

some aspects of biometric information

https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-personal-information/#SensitiveInfo

Consent

Generally, sensitive information has a higher level of privacy protection than other personal information. Consent to collection and use is usually required: APP 3.3.

Checking your understanding of privacy law

X provides robo cypto trading advice. X wants to collect name, email, age, address, and biometric information. Can X do this? If so how? Can X sell this information to a credit rating service?

Y runs an independent supermarket. Y wants to collect faceprints from shoppers entering the store. Can Y do this? If so how? Can Y use this information for marketing?

Z is a real estate agent. Z collects name, age, employer, income, educational qualifications, drivers licence and passport information. Can Z do this? If so how? Can X use this information for research purposes?

GDPR Article 6: Lawful basis for processing

(a) Consent

(b) Contract

(c) Legal obligation

(d) Vital interests

(e) Public task

(f) Legitimate interests

GDPR: Individual rights

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

3. General law

For example:

- Admin law
- Business law
- Criminal law

Principles Based Regulation

Old law applied to new problems, or

Too slow and rigid?

4. Specific law for AI

Problems or hurdles unique to AI

↓

'Ex ante' regulation

California bot law	EU AI draft Law

用chatbot 回答用户 必须告知用户（事先告知）

EU Draft AI Law

Risk based categories

Exhibit 1

The European Union's draft AI regulations classify AI systems into three risk categories.

Unacceptable-risk AI systems	High-risk AI systems	Limited- and minimal-risk AI systems
• Subliminal, manipulative, or exploitative techniques causing harm • Real-time, remote biometric identification systems used in public spaces for law enforcement • All forms of social scoring	• Systems that evaluate consumer creditworthiness • Recruiting or employee-management systems • Systems utilizing biometric identification in nonpublic spaces • Safety-critical systems (eg, systems that would put the health of citizens at risk due to failure) • Any systems used in the administration of justice	• AI chatbots • AI-enabled video and computer games • Spam filters • Inventory-management systems • Customer- and market-segmentation systems • Most other AI systems

McKinsey & Company

EU AI Act: Obligations

Exhibit 2

The draft EU AI regulations place several requirements on organizations providing or using high-risk AI systems.

- ☑ Implementation of a risk-management system
- ☑ Data governance and management
- ☑ Technical documentation
- ☑ Record keeping and logging
- ☑ Transparency and provision of information to users
- ☑ Human oversight
- ☑ Accuracy, robustness, and cybersecurity
- ☑ Conformity assessment
- ☑ Registration with EU-member-state government
- ☑ Postmarket monitoring system

McKinsey & Company

Case studies

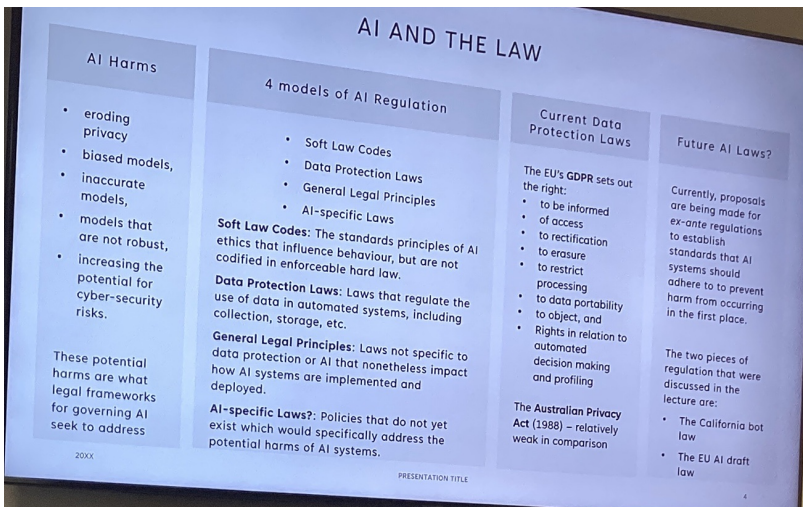
Technology	Risk	AI Principles	Privacy	EU AI
Facial recognition technology	inaccurate affect job privcy erodig	dissable the process		public places not be allowed in
Automated employment tool				
ChatGPT	low accuracy misleadg injure reputatio		misuse private informatio	low risk
Paro the robot seal				

hard law is change slowly soft law is flexible, more and update quickly

THE UNIVERSITY OF MELBOURNE

Thank you

Melbourne Law School


AI AND THE LAW
AI Harms
eroding privacy
biased models,
inaccurate models,
models that are not robust,
increasing the potential for cyber-security risks.
These potential harms are what legal frameworks for governing AI seek to address
4 models of AI Regulation
Soft Law Codes
Data Protection Laws
General Legal Principles
AI-specific Laws
Soft Law Codes: The standards principles of AI ethics that influence behaviour, but are not codified in enforceable hard law.
Data Protection Laws: Laws that regulate the use of data in automated systems, including collection, storage, etc.
General Legal Principles: Laws not specific to data protection or AI that nonetheless impact how AI systems are implemented and deployed.
AI-specific Laws?: Policies that do not yet exist which would specifically address the potential harms of AI systems.
Current Data Protection Laws
The EU's GDPR sets out the right:
to be informed
of access
to rectification
to erasure
to restrict processing
to data portability
to object, and
Rights in relation to automated decision making and profiling
The Australian Privacy Act (1988) – relatively weak in comparison
Future AI Laws?
Currently, proposals are being made for ex-ante regulations to establish standards that AI systems should adhere to to prevent harm from occurring in the first place.
The two pieces of regulation that were discussed in the lecture are:
The California bot law
The EU AI draft law
20XX
PRESENTATION TITLE
4