Ethical AI

IEEE Ethical Considerations in AI/AS

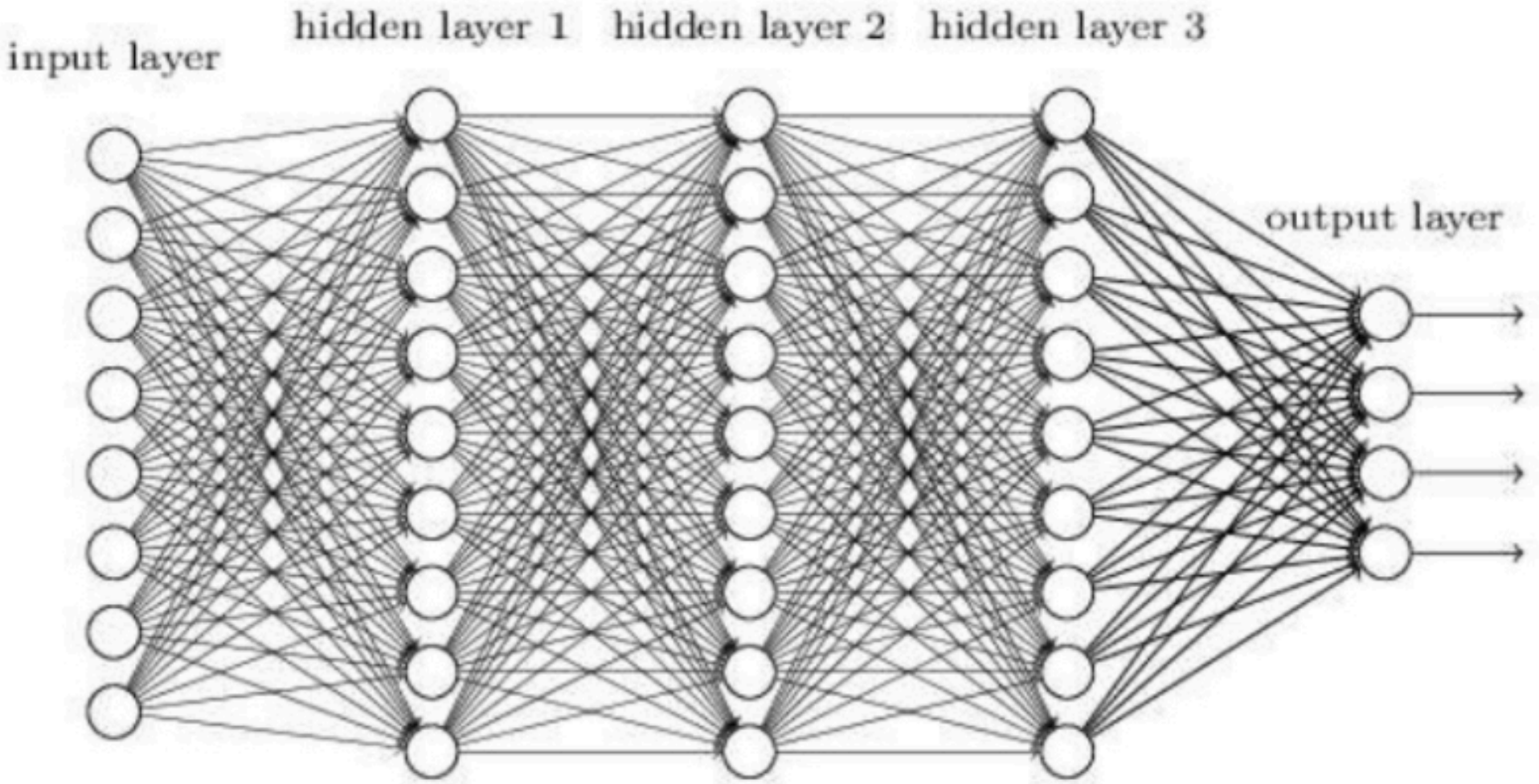
Kenny Huang, Ph.D. 黃勝雄博士

Executive Council Member, APNIC 亞太網路資訊中心董事

Board, Mind Extension

huangksh@gmail.com

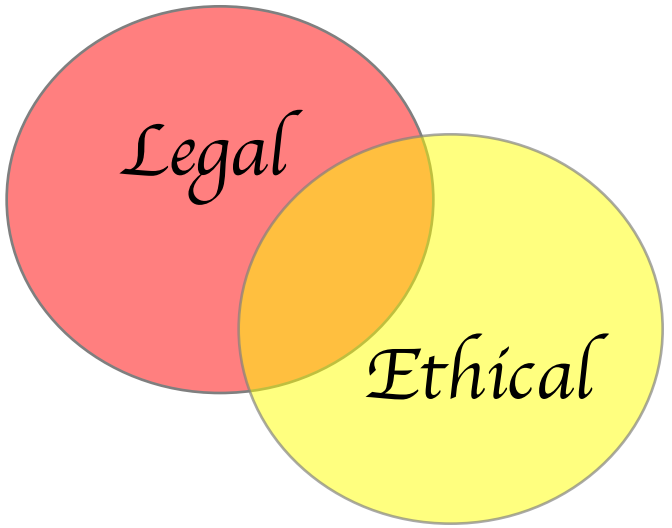
Oct 13 2017



No one truly understands on the theoretical basis why deep neural networks provide good result

- All automated decision making system display bias !
  - ✓ The question is : Is it unfair, unethical or illegal bias

- Lot of laws allow unethical
  - ✓ Abortion laws



Utilitarian orientated perspective	Kantian/Rights Based perspective
My data is a resource to be harvested and put to use	My data is a part of who and what I am. It's mine!
Constraints (laws) to prevent specific abuses and misuse of my data	My data should be treated with respect, just as I expect to be treated with respect
Better data & predictions = better outcomes. Everyone benefits.	I will decide how data about me is used. You have no right to use my data without my permission

Policy for Personal Data and Individual Access Control (IEEE)

- Allows every global citizen/individual access to tools allowing them control over a minimum common denominator of attributes that define his/her identity.
- Allows the possibility for citizens/individuals to access, manage, and control how their data is shared.
- Provides easily understandable ways for citizens/individuals to choose how or whether to share their data with other individuals, businesses, or for the common good as they choose.
- Provides for future educational programs training all citizens/individuals regarding the management of their personal data and identity, just as many countries provide training in personal finances and basic legal understanding.

Personal Data Definitions

- Q: How can an individual define and organize his/her personal data in the algorithmic era?
  - Where available individuals should identify trusted identity verification resources to validate, prove, and broadcast their identity
  - e.g., eIDAS; IDNYC
- Q: What is the definition and scope of personally identifiable information
  - EU Data Protection Directive 95/46: personal data as "any information relating to an identified or identifiable natural person."
  - PII should be considered the sovereign asset of the individual to be legally protected and prioritized universally in global, local and digital implementations

- Q: What is the definition of control regarding personal data
  - Most individuals believe controlling their personal data only happens on the sites or social networks to which they belong.
  - Personal data should be managed starting from the point of the user versus outside actors having access to data outside of a user's awareness or control.

Personal Data Access and Consent

- Q: How can we redefine data access to honor the individual?
  - Practical and implementable procedures need to be available in order for designers and developers to use “Privacy-by-Design”/Privacy-by-Default methodologies
- Q: How can we redefine consent regarding personal data so it honors the individual?
  - In order to realize benefits such as decision enablement and personalization for an individual, open standards and interoperability are vital to ensure individuals and society have the freedom to move across ecosystems
- Q: Data that appears trivial to share can be used to make inferences that an individual would not wish to share.
  - While it is hoped AI/AS that parse and analyze data could also help individuals understand granular level consent in real-time, it is imperative to also put more focus on the point of data collection to minimize long-term risk.

Privacy by Design

- 7 Principle
  - Proactive not reactive
  - Privacy as the default
    - purpose specification; collection limitation; data minimization; use, retention and disclosure limitation
  - Privacy embedded into design
  - Full functionality
  - End-to-end security - full lifecycle protection
    - ensure confidentiality; integrity and availability
  - Visibility and transparency - keep it open
    - accountability; openness; compliance
  - Respect for user privacy - user centric
    - consent; accuracy; access; compliance

- Q: How can data handlers ensure the consequences (positive and negative) of accessing and collecting data are explicit to an individual in order for truly informed consent to be given?
  - To guard against these types of complexities we need to make consent both conditional and dynamic. Safeguards are required to surface the downstream impact of data that appears to be trivial that can be later used to make inferences that an individual would not wish to share.

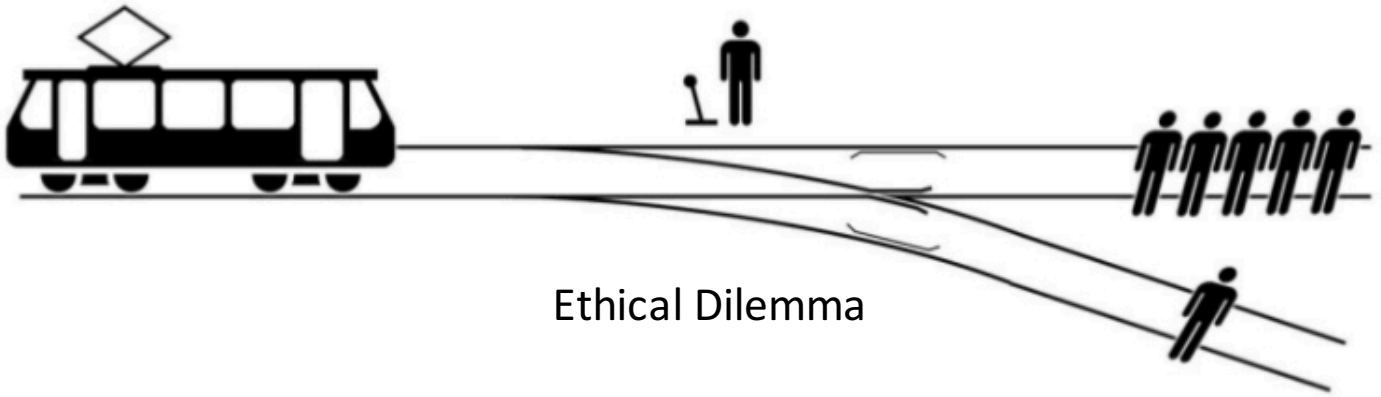
Personal Data Management

- Q: Could a person have a personalized AI or algorithmic guardian?
  - Algorithmic guardian platforms should be developed for individuals to curate and share their personal data.
  - Such guardians could provide personal information control to users by helping them track what they have agreed to share and what that means to them while also scanning each user's environment to set personal privacy settings accordingly.

How can we assure that AI are **accountable** ?

How can we assure that AI are **transparent** ?

How can we extend the benefits and **minimize** the risk of AI technology being **misused** ?



Ethical Dilemma