AI Regulation
CloudCamp, 11 Sept 2024

Dr W Kuan Hon

(personal views only !)

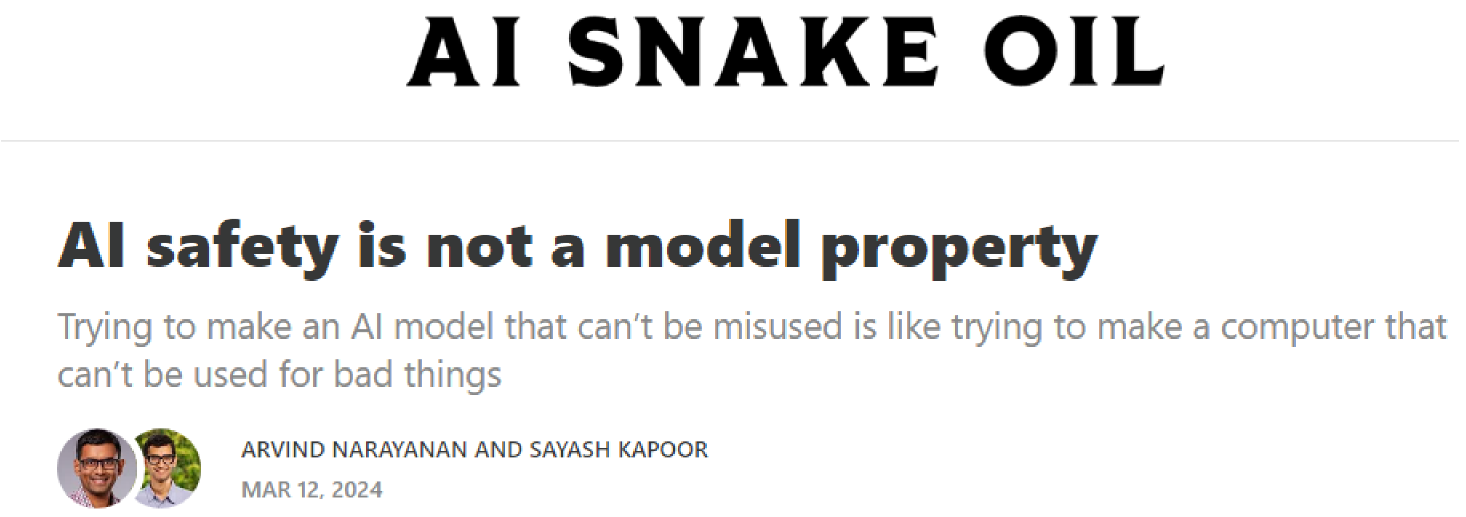
https://www.kuan0.com

https://www.linkedin.com/in/wkhon/

Multi-purpose / dual-use tech: policy ?

Tech neutrality:
Regulate tech’s
usage / purpose

Regulate a specific technology as such ?



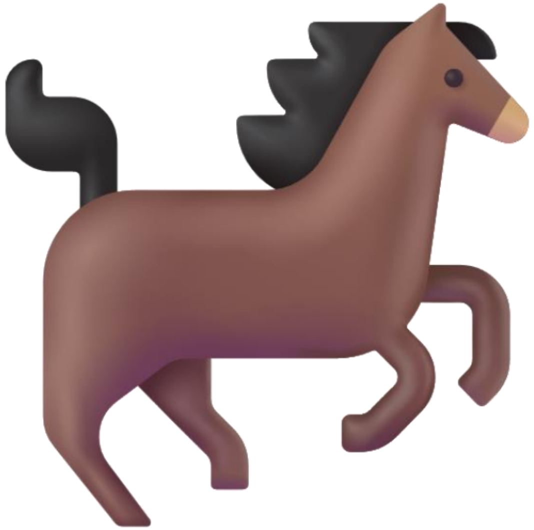
AI SNAKE OIL

AI safety is not a model property

Trying to make an AI model that can’t be misused is like trying to make a computer that can’t be used for bad things

ARVIND NARAYANAN AND SAYASH KAPOOR
MAR 12, 2024

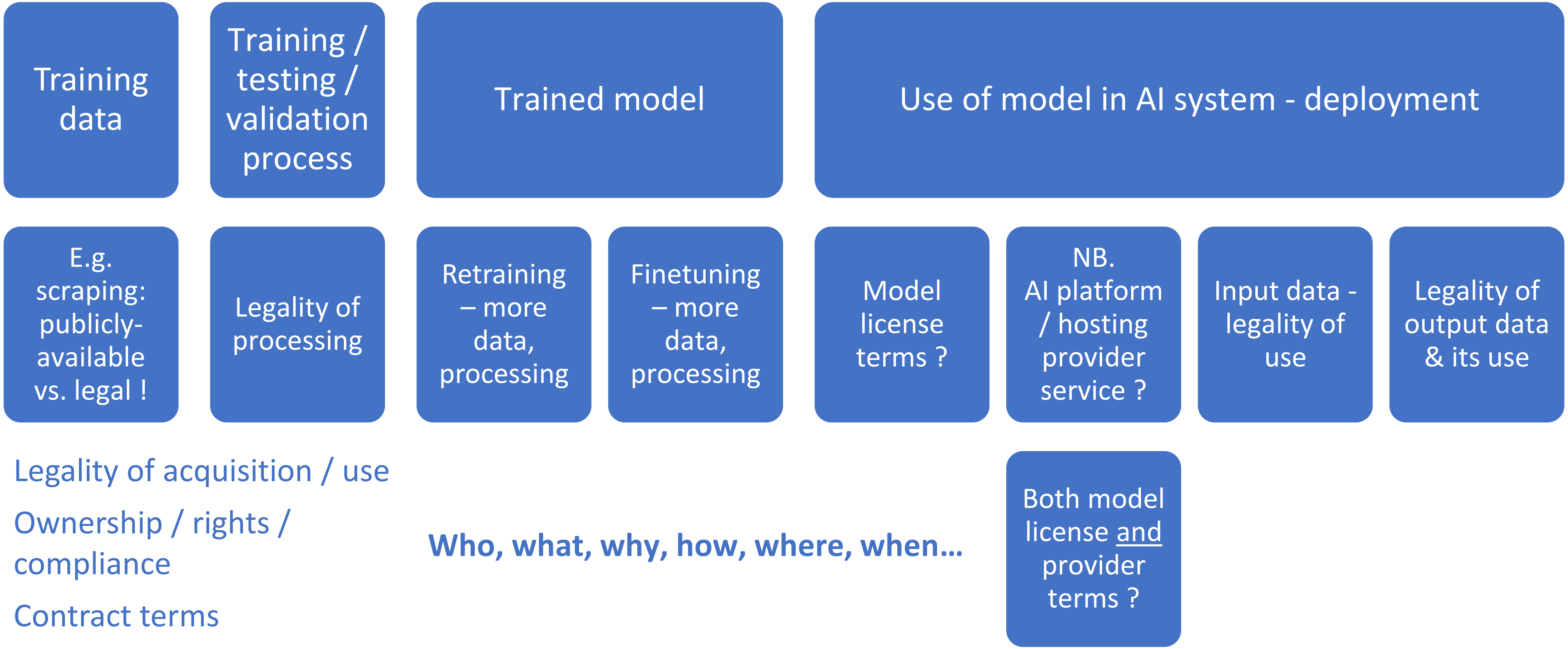
AI-specific and other laws…



- AI-specific laws / regulation
  - US EO14110 + state laws: Colorado, California? etc.
  - EU AI Act; AI liability, product liability, etc
  - UK - “companies developing the most powerful AI models…”
  - More jurisdictions…

- Non AI-specific legal issues already affect AI development / use, e.g.:
  - Intellectual property - copyright, patents; ownership, licensing
  - Data protection / privacy - e.g. ADM, scraping, training, explainability
  - Defamation
  - Equality - e.g. facial recognition accuracy
  - Competition / anti-trust
  - Contracts / licences - AI / model providers; open source ? vs. docs / webpages

ML lifecycle - legal issues throughout



Training data

E.g. scraping: publicly-available vs. legal !

Training / testing / validation process

Legality of processing

Trained model

Retraining – more data, processing

Finetuning – more data, processing

Use of model in AI system - deployment

Model license terms ?

NB. AI platform / hosting provider service ?

Both model license and provider terms ?

Input data - legality of use

Legality of output data & its use

Legality of acquisition / use

Ownership / rights / compliance

Contract terms

Who, what, why, how, where, when…

Many, many legal issues / uncertainties

Extraterritoriality
e.g. GDPR, also AI Act…

E.g. ops in EU, output used in EU

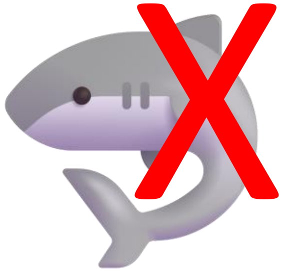
🪝 Jurisdiction, but reputation / trust… 🤝 💰 📉

Other legal uncertainties, e.g. EU AI Act alone… definitional problems

- Lists of “prohibited”, “high-risk”, limited-risk (transparency) but… & outside scope
- Tech stack / supply chain complexities:
    - AI model, “GPAI model”, “AI system”, AI product, downstream system…
    - Hosting / AI management platforms - contract terms (model license terms)
    - Roles - deployer, provider, importer, manufacturer, distributor…

Legal risks

- Fines, class-action lawsuits, suspend / halt operations or even business
- Reputational risk
- Personal risk to employees, e.g. on security front
- Legal risks, like security…
  - Should NOT be an afterthought
  - Are a journey, not a destination ✈️
- Involve legal / privacy experts !
  - At outset, cf. “quick scan” day before launch 🙄 😭 ✋❌
  - Throughout projects’ lifecycle, including post-deployment monitoring
  - Cross-functional teams



Thank you ! 🙏

Dr W Kuan Hon (personal views only !)
https://www.kuan0.com
https://www.linkedin.com/in/wkhon/

Extraterritoriality

🎵 🧑‍🌾 Old MacDonald had a thought, E-U-A-I-O !
Could AI Act apply or not ? E-U-A-I-O !
If his output's used in the EU, yes
Many other aspects extraterritorial
Old MacDonald, check your role(s), E-U-A-I-O !