CMS
law·tax·future

WHERE ARE THE LEGAL BOUNDARIES FOR AI TOOLS?

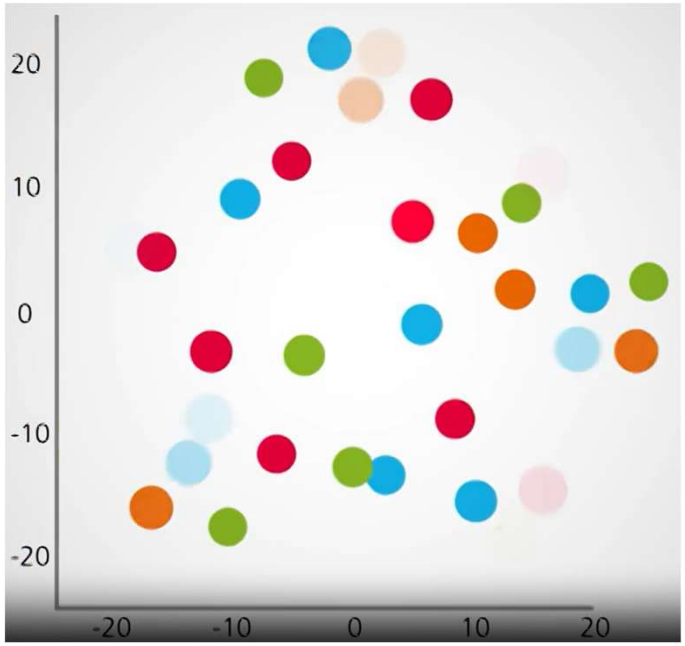
WHITE PAPER DEFAMATION CONFERENCE
18 NOVEMBER 2025

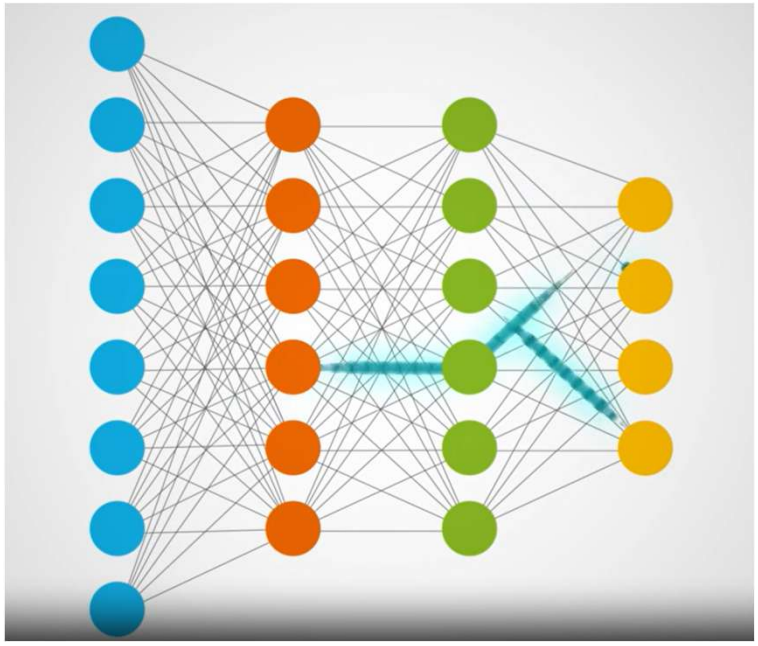
TO BE COVERED TODAY

- How AI works
- Legal use cases
- Regulatory position
- Litigation risks
    - Copyright
    - Defamation
    - Data protection
    - Discrimination
    - Contract

HOW AI WORKS

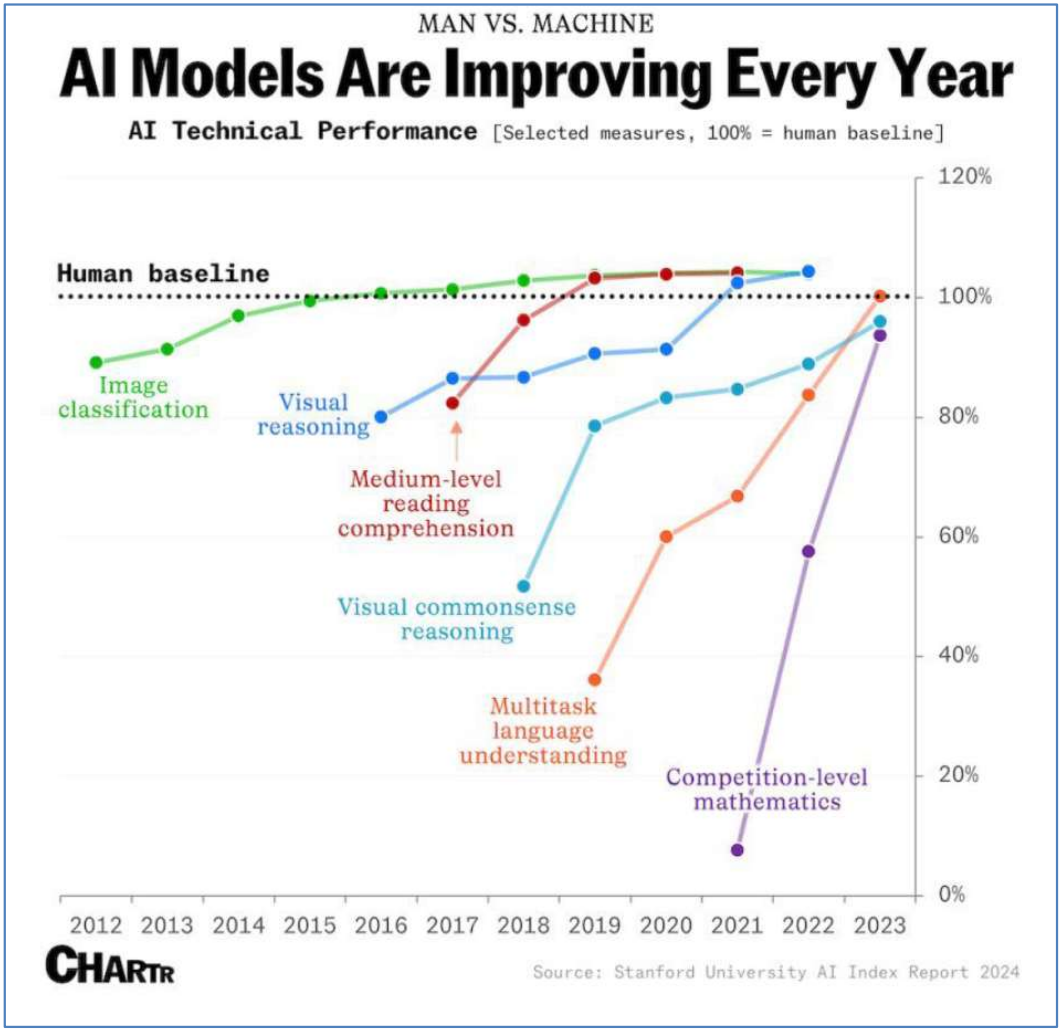
- Transformer
  - “Attention Is All You Need” - Google 2017
- Neural network, matrix multiplication
- Training
- Chat GPT4: said to have 1.8b parameters, 120 layers
- Grok-4: said to have 2b parameters, probably around 120 layers





KEY AI ISSUES

- No-one can tell how any output was achieved
- No-one can tell what any result will be
- Hugely improving performance – “human reference factor”
- Hallucinations / poisoning
- Copying / confidentiality



LITIGATION USE CASES

- Document review
- Meeting notes / summaries
- Managing tasks / cost management / fee estimates
- Identifying inconsistencies
  - In court
- Drafting documents
  - Facilitating litigants in person
- Identifying AI generated material
- Determining cases
  - Expert selection
  - Judge / counsel analysis

UK REGULATORY APPROACH

Legislative and Policy Background

- National AI Strategy (22 September 2021)
- AI White Paper: a Pro-Innovation Approach to AI Regulation (29 March 2023, reaffirmed in February 2024)
- Artificial Intelligence (Employment and Regulation) Bill (18 April 2024)
- Automated Vehicles Act 2024

Cross-sectoral oversight

- DSIT: Department for Science, Innovation and Technology
- AI Safety Institute
- AI Standards Hub
- Digital Regulation Co-operation Forum
- Responsible Technology Adoption Unit

Regulators' approach to AI

- Bank of England and PRA
- Competition and Markets Authority Strategic AI Update (
- Financial Conduct Authority AI Update (22 April 2024)

Governance, data laws and more…

- Data (Use and Access) Bill
- Consultation on AI Management Essentials tool (DSIT):
- Overlaps with data protection law: UK ICO data protection and AI toolkit, UK GDPR Article 22.

CATEGORISE ROLE UNDER EU AI ACT AND UNDERTAKE RISK CLASSIFICATION

Providers, deployers, importers, and distributors of systems that meet that description need to consider whether those systems further qualify as ‘high-risk’ AI systems.

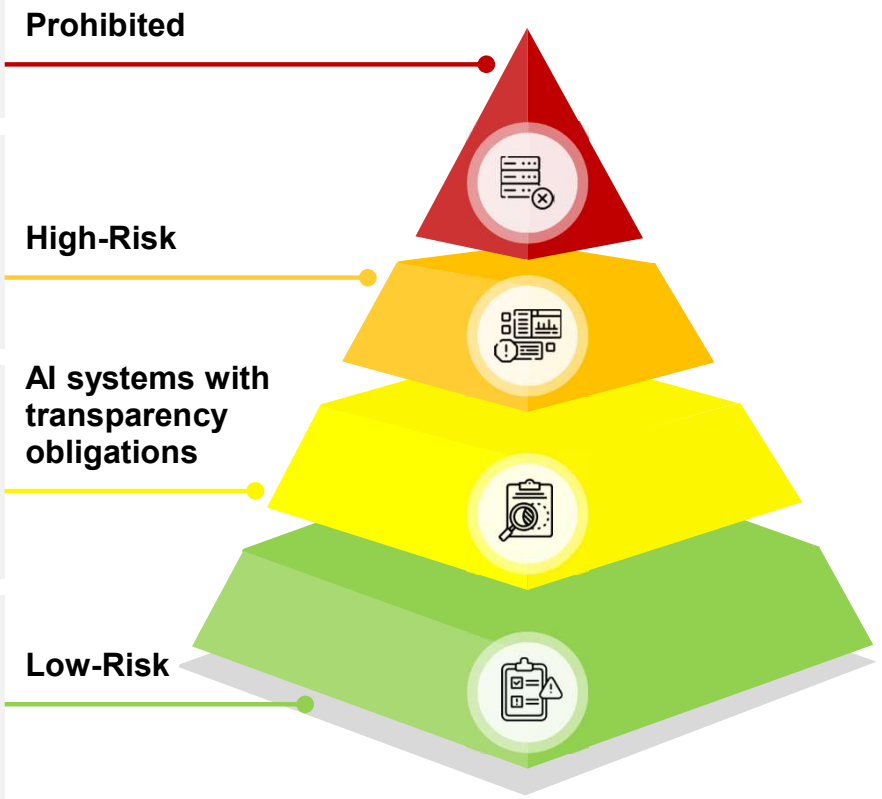
Identifying AI system usage and classifying AI systems according to risks is an important first step towards understanding EU AI Act compliance obligations. AI systems can be evaluated by regulators and re-classified, and there is also a risk of systems changing purpose, and therefore classification treatment, over time. High penalties would apply to those not complying with updates.

Prohibited
Systems considered to create a threat to safety and rights, including social scoring or applications that encourage harmful behaviors. These should be discontinued immediately.

High-Risk Systems
Specific rules apply to AI systems that create a high risk to the health and safety or fundamental rights of natural persons. This includes systems that make recruitment decisions or evaluate creditworthiness

Transparency Risk Systems
An obligation to disclose use of AI is imposed on some systems which have specific risks of manipulation, e.g., systems interacting with humans and used to detect emotions, generate/manipulate content.

Minimal Risk Systems
Other uses of AI are not specifically classified, but some compliance responsibilities still apply. This includes a general duty of AI literacy, non-high risk system assessment, codes of conduct, responsible practices and industry standards



AI LITERACY

- Article 4 of the EU AI = a duty on both providers and deployers of AI systems to ensure a sufficient level of AI literacy
- Relates both to staff and other persons dealing with the operation and use of AI systems, i.e. potentially contractors or supply chain actors (outsourced services)
- Obligation applies irrespective of the types of AI system being deployed: so, including where systems are not high risk or transparency risk systems
- Broad definition of AI System: the duty will apply to most organisations using automation software
- In effect from February 2025 but enforcement does not begin until October 2025

EU AI ACT TIMELINE – WHEN SHOULD YOU BE COMPLIANT

Application to non-EU businesses

The AI Act could apply if your organisation places an AI system on the EU market or puts AI systems into service in the EU, or if the system's output is used in the EU, regardless of where your business is established. It is important to know your role under the Act and how your activities are classified.

Today

1 August 2024

The EU AI Act officially entered into force across all 27 EU Member States.

2 February 2025

Ban on Prohibited Systems in effect

AI literacy training requirements also start to apply

2 August 2025

Penalties, along with the rules on General Purpose AI take effect

2 August 2026

Fully applicable

The Act is expected to be fully applicable, with all provisions enforced.

2 August 2027

Rules on high-risk systems used as safety components become applicable

Penalties apply for non-compliance

Tiered penalties, with maximum EUR35m or 7% total worldwide annual turnover (whichever is highest)

In addition, there may be reputational impact, and authorities may impose corrective measures, such as requiring changes to AI systems or halting deployment, and expensive remediation projects

LITIGATION REGARDING AI

- IP / copyright
- Defamation
- Data protection
- Discrimination
- Contractual disputes

COPYRIGHT – UK POSITION

- The LLM training process
  - Ingesting copyright works
  - Training LLM model
  - Production of AI material
  - Where do these acts take place

- UK Government consultation
  - Consultation "Copyright and Artificial Intelligence" issued December 2024
  - Establishment of Working Groups July 2025

COPYRIGHT - *GETTY IMAGES V STABILITY AI*

- *Getty Images v Stability AI* [2025] EWHC 2863
- The trademark claim

COPYRIGHT - *GETTY IMAGES*

- The copyright claim

  > "In reality therefore, the dispute between the parties as it finally emerged in closing, really turns on whether an article whose making involves the use of infringing copies, but which never contains or stores those copies, is itself an infringing copy such that its making in the UK would have constituted an infringement. Taking the specific facts with which I am concerned, is an AI model which derives or results from a training process involving the exposure of model weights to infringing copies itself an infringing copy. Para 599"

- Two questions.
  - Is the AI output an "article"?
  - Is the AI output an "infringing copy"?

COPYRIGHT - *GETTY IMAGES*

"In reality therefore, the dispute between the parties as it finally emerged in closing, really turns on whether an article whose making involves the use of infringing copies, but which never contains or stores those copies, is itself an infringing copy such that its making in the UK would have constituted an infringement. Taking the specific facts with which I am concerned, is an AI model which derives or results from a training process involving the exposure of model weights to infringing copies itself an infringing copy?

In my judgment, it is not … While it is true that the model weights are altered during training by exposure to Copyright Works, by the end of that process the Model itself does not store any of those Copyright Works; the model weights are not themselves an infringing copy and they do not store an infringing copy…

I agree with Stability that the concept of an infringing copy cannot be interpreted in the abstract without reference to the fundamental nature of a copy…"

Paras 599 to 601

COPYRIGHT - INTERNATIONALLY

- US
  - Fair use defences are typically succeeding:
    - *Bartz v. Anthropic* PBC, 3:24-cv-05417
      - $1.5 billion class settlement for piracy claims
    - *Kadrey v. Meta Platforms*
  - We await *The New York Times v. OpenAI*

- Europe
  - Digital Single Market Directive
  - We await *Like Company v. Google Ireland* at the CJEU

DEFAMATION

- Responsibility for publication.
- The section 1 issue:

  "A statement is not defamatory unless its publication has caused or is likely to cause serious harm to the reputation of the claimant." Section 1(1), Defamation Act 2013.

  [The Claimant] complains of the publications to individuals; that is why I was surprised to see that you have a single serious harm paragraph. Each of [the] publications is a separate cause of action, and it must be supported in its own way by … proof of serious harm caused by that publication.

  Nicklin J, *Amersi v Leslie & Anor*

- Undertakings not to repeat. Filter: prompts; ingested data; output?
- Malice?
- Intermediary defences.

DATA PROTECTION

- Fair processing.
- Automated decision-making

  "The data subject shall have the right to obtain from the controller …

  …

  (h) the existence of automated decision-making [and] meaningful information about the logic involved…"

  Article 15(1) UK GDPR

  "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

  Article 22(1) UK GDPR

- *ICO v Clearview AI* [2025] UKUT 319

DISCRIMINATION

- *Manjang v Uber Eats UK Ltd* and others: 3206212/2021
  - Facial recognition was said to be racially discriminatory
  - Case settled
- *R (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058

  > "The algorithms of the law must keep pace with new and emerging technologies."
- *JCWI v Home Office* - algorithmic visa processing
- *PLP v Home Office* - sham marriage algorithm

CONTRACT

- No significant contractual cases yet re AI.
- Main issue likely to be defining contractual performance.
  - *Tyndaris v VWM*