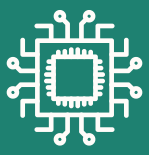
AI OPENNESS:
A PRIMER FOR POLICYMAKERS

The OECD report titled "AI Openness: A Primer for Policymakers" (August 2025, No. 44) is an international policy document addressing the legal implications of open-weight foundation models.

This infographic summarizes the key findings of the report for legal professionals, with particular focus on licensing uncertainties, liability issues, and intellectual property/personal data protection risks.

DIFFERENCES BETWEEN OPEN SOURCE AND "OPEN SOURCE" AI

Open Source Software		"Open Source" AI
Source code is **completely open:** Viewable, modifiable, distributable. License terms are clear and predictable.	**BASIC DEFINITION** 	Term is often misleading. Model weights are not source code. Components may be transparent piece by piece.
Single component: Source Code	**COMPONENTS** 	**Different components:** Training Code Inference Code Model Weights Training Data
License terms are clear. Copyright protection is well-defined. Liability framework is specific.	**LEGAL FRAMEWORK** 	Software licenses are not suitable. Intellectual property is uncertain. Liability boundaries are ambiguous.

OPEN-WEIGHT MODELS

OECD prefers to use the term "open-weight model" instead of "open source" AI.

- **A clearer and non-misleading term.**
- **Indicates that only the weights are open.**
- **Does not create false assumptions about license, data, or code.**

WHERE DO OPEN-WEIGHT MODELS FIT WITHIN ALL AI MODELS?

ALL AI MODELS

Foundation Models
General-purpose, large models
Examples: GPT-4, Claude, LLaMA, Stable Diffusion

← OECD Report focuses here

AI Models
Examples: Spam filters, face recognition, voice recognition

Model Openness Framework (MOF)
A framework by the Linux Foundation for evaluating openness levels across all AI models (Classes I-III)

OPEN-WEIGHT MODELS

BENEFITS

Innovation and Research
Development of new applications and products, access for scientific research and technical advancement, development efficiency and cost savings.

External Audit and Accountability
Independent experts can evaluate model performance. Detection of errors and biases.

Competition Law Perspective
Reduction of market entry barriers, prevention of monopolization, talent development and digital equity.

Control and Accessibility
Sensitive data management: Public and private sector can process sensitive data locally without sending to third parties, compliance and explainability research.

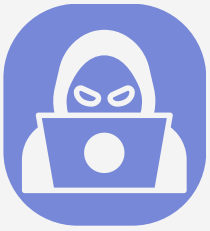
RISKS

Intellectual Property Violation
Unauthorized use of copyrighted content in training data, extraction of original works from model weights.

Data Protection Violation
Personal data in model weights, right to erasure cannot be applied, membership inference attacks.

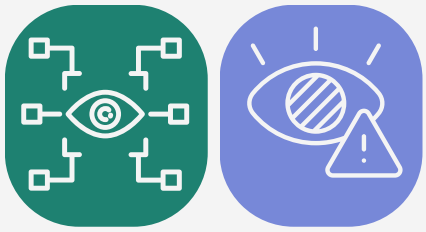
Developer Liability and Loss of Control
Original developer's liability is ambiguous for harmful use with open models, uncontrolled proliferation.

Cyberattacks
Advanced phishing, malicious software, use for unauthorized access to information systems, removal of original security layers and filters.



Digital Security Testing

Red teams can legally test potential attack scenarios, improving digital security and safeguards, preventing unwanted and harmful behaviors.



CSAM and NCII

Use of open-weight image generation models to produce child abuse and non-consensual intimate content.

WHY IS ALL THIS IMPORTANT FOR LEGAL PROFESSIONALS?

Uncertainties in Licensing Law

- Traditional open-source software licenses cannot be directly applied to AI model weights.
- Necessity of developing new license types.
- Need to interpret existing licenses (Apache 2.0, MIT, Creative Commons) in the AI context.

Liability and Accountability

- Open-weight models can be easily reconfigured by malicious actors.
- Developer's original security measures can be bypassed.
- Makes determination of legal liability extremely difficult.
- Difficulty of recalling the model from the market.

Intellectual Property (IP) & Data Privacy Law

Adopting open-weight models instead of closed models offers:

- advantages for public institutions and businesses with sensitive data,
- no sharing of data with third-party vendors,
- compliance with data sovereignty and privacy regulations.

However, open-weight models present distinct intellectual property risks:

- Models may memorize and leak copyrighted material from their training data.
- Once weights are public, developers lose control over preventing copyright violations in downstream uses.

Risk Assessment and Regulatory Compliance

Decisions regarding AI openness must be addressed within a **holistic risk assessment framework** that evaluates marginal risks and benefits by comparing open-weight models to closed alternatives and existing technologies.

Source: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/08/ai-openness_958d292b/02f73362-en.pdf

Content:
Att. Özden Serinay Öz
Att. Rümeysa Kırpat

Design: Att. Ayşenur Kölgesiz

Istanbul Bar Association
Information Technology Law Commission
Artificial Intelligence Working Group