

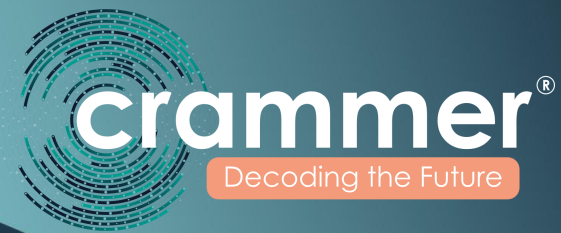


# crammer<sup>®</sup>

Decoding the Future

## WELCOME!

# PLENARY ROOM



## Speakers



Darren Olivier



Lita Miti-Qamata



Mandla Ngidi



Danielle van Deventer

## AI and IP: From Legal Uncertainty to Operational Readiness

What has changed since 2025 | Where the legal uncertainty still sits | How to become operationally ready now





AI is moving faster than the law.

This session is not about predicting outcomes in law, but it is about understanding exposure and what to do about it.

- AI/IP uncertainty is not resolved
- Risk has shifted from theory



## Risk categories:

- Loss of IP ownership
- Infringement Liability
- Reputational Damage
- Regulatory Sanctions/Compliance failures
- Ethical misconduct

See: Tab 2 [www.smartaiip.adams.africa](http://www.smartaiip.adams.africa)

# Today's flow (4 speakers)

- ▶ **Lita:** key US/UK developments (Anthropic; Getty/Stability)
- ▶ **Mandla:** AI and privilege (US)
- ▶ **Danielle:** Africa governance + SA reputational-risk lessons
- ▶ **Darren:** summary + SmartAI IP Readiness Test + next steps

As you listen to the next three speakers, I want you to keep one question in mind:

**"if this happened in your organisation tomorrow, would you know that the organisation owns the risk; who was authorised to deploy or create AI in that way; and what evidence would you point to, to show that the risk is governed, not accidental?"**

However, it is also about value enhancement, and I will explain that at the end.

# Copyright Lawsuits v. AI Companies

## Canada



**CanLII v. Caseway AI**  
Supreme Ct. of British Columbia



**Toronto Star News. v. OpenAI**  
Ontario Superior Ct. of J.

## UK



**Getty Images (US) v. Stability AI Ltd.**  
High Court of Justice in London

## Netherlands



**DPG Media v. HowardsHome:** TDM exception  
Amsterdam Dist. Court

## France



**National Publishing Union v. Meta**  
Tribunal Judiciaire de Paris

## Germany



**GEMA v. OpenAI**  
Munich Regional Court  
**GEMA v. Suno**  
Munich Regional Court



**Kneschke v. LAOIN**  
Hamburg Regional Court

## South Korea



**Korean Broad. Assn. v. Naver**  
Seoul Central Dist. Court

## China



**Shanghai Character License Administrative Co. v. TAB**  
Guangzhou Internet Court

## India



**Asian News Int'l. v. OpenAI**  
New Delhi Court

## Copyright + Related Lawsuits v. AI Companies

### ND California

- Kadrey v. Meta; Chabon v. Meta; Huckabone v. Meta; Earnsworth  
Judge Chhabria
- In re OpenAI ChatGPT Litigation (Tremblay, Silverman, Chabon)  
Judge Araceli Martinez-Olguin
- Nazemian v. NVIDIA Corp., Dubus v. NVIDIA Corp. (related)  
Judge Tiger
- In re Mosaic LLM Litigation (O'Neil, Mahall)  
Judge Breyer
- Bartz v. Anthropic, Judge Alsop
- Concord Music v. Anthropic  
Judge Lee
- Doe 1 v. GitHub, Microsoft, OpenAI  
Judge Tiger
- Sarah Andersen v. Stability AI; Deviant Art, Midjourney, Runway AI  
Judge Orrick
- In re Google Gen. AI Litig. (Zhang, Leoni)  
Judge Lee
- Brain Software v. News Corp.  
Judge Breyer

### D. Col.



Pierce v. Photobucket  
Judge Brommer

### D. Mass.



UMG Recordings v. Suno  
Chief Judge Taylor IV

### SDNY

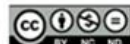
- Authors Guild v. OpenAI; Alter, Basbanes  
Judge Stein
- New York Times v. OpenAI  
Daily News v. Microsoft  
Center for Inv. Res. v. OpenAI  
Judge Stein
- Huckabone v. Bloomberg  
Judge Garmett
- Dow Jones v. Parolexity AI  
Judge Polk Falla
- Advance Loc. Media v. Cohere  
Judge TSD
- Raw Story v. OpenAI  
Judge McMahon
- Intersect v. OpenAI  
Judge Rakoff
- UMG Recordings v. Uncharted Labs d/b/a Udio  
Judge Hellerstein
- Leibman v. Lorch  
Judge Otkien

### Delaware

- Yackey v. Eleven Labs  
Judge Andrews
- Thomson Reuters v. ROSS Intell.  
Judge Bibas
- Getty Images v. Stability AI  
Judge Hall

### CD California

- Alcon Ent. v. Tesla  
Judge Oliver



# United States v Heppner

## ***You might lose legal privilege through use of AI, who would have thought?***

- ▶ This case highlights how everyday use of AI can quietly destroy privilege.
- ▶ Heppner used Anthropic AI tool “Claude” to generate documents for a legal strategies. All this exercise was done without direction of an attorney and without first consulting an attorney.
- ▶ When Heppner’s documents were seized, he attempt to claim attorney – client privilege.
- ▶ The court found that privilege cannot be claimed on the reasons that:
  - (a) Communication was not between the client and attorney;
  - (b) There was no confidentiality (as the terms of service for Claude allowed for disclosure of information to government regulators, with that the user could not have reasonable expectation of confidentiality);
  - (c) Legal advice was not sought from a lawyer but from an AI tool; and
  - (d) Sharing the AI output with a lawyer after the facts did not create privilege.



# Continues...

- ▶ The South African courts would have dealt with the case the same way the US court handled it.
- ▶ In South Africa, legal privilege requires the interaction between a client and attorney to be linked with the legal advice or litigation advice. In light of this, it is unlikely that our courts would not have taken a different decision to that of the US court.
- ▶ Accordingly, for any interaction to enjoy protection from discovery, it is important that such engagements must be between an (practicing) attorney and client.
- ▶ The takeaway from this case is that “**governance failures do not show up when you purchase the AI tool, but they show up when you are already in trouble**”.

# AI Policy Landscape in Africa

| African Union (AU) | Continental AI Strategy endorsed July 2024, guiding 2025–2030 national adoption                                                                        |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kenya              | National AI Strategy 2025–2030 launched 27 March 2025                                                                                                  |
| Zambia             | National AI Strategy 2024–2026 launched Nov 2024                                                                                                       |
| Cameroon (OAPI)    | National AI Strategy (SNIA) launched Jul 2025 with seven pillars incl. “GPT Cameroon”, edge computing, data governance, talent & research.             |
| South Africa       | Draft National AI Policy Framework published 25 Oct 2024;<br>King V – Principle 10                                                                     |
| Ghana              | National AI Strategy finalised (early 2026) with launch pending                                                                                        |
| Mozambique         | No AI Act yet; UNESCO supported National AI Strategy work underway (late 2025).                                                                        |
| Mauritius          | Digital Transformation Blueprint 2025–2029 integrates AI/data pillars; refreshed National AI Strategy in development (2025 stakeholder consultations). |
| Nigeria            | Draft National AI Strategy (NAIS) released August 2024; still not adopted.                                                                             |
| Rwanda             | National AI Policy (Apr 2023) actively implemented through 2024–2026.                                                                                  |

# AI in African Courts: Real Cases, Real Risks

Courts are already policing AI—through real cases.

## ▶ South Africa:

- ▶ *Philani Godfrey Mavundla v MEC: Department of Co-Operative Government and Traditional Affairs, KwaZulu-Natal and Others [2025] ZAKZPHC 2 (KwaZulu-Natal Division, Pietermaritzburg, 8 January 2025)*
- ▶ *Northbound Processing (Pty) Ltd v South African Diamond and Precious Metals Regulator and Others, unreported case no. 2025/072038 (30 June 2025)*

▶ **Kenya** (Supreme Court, 2025): Justice Lenaola advised avoiding AI until guidelines exist.

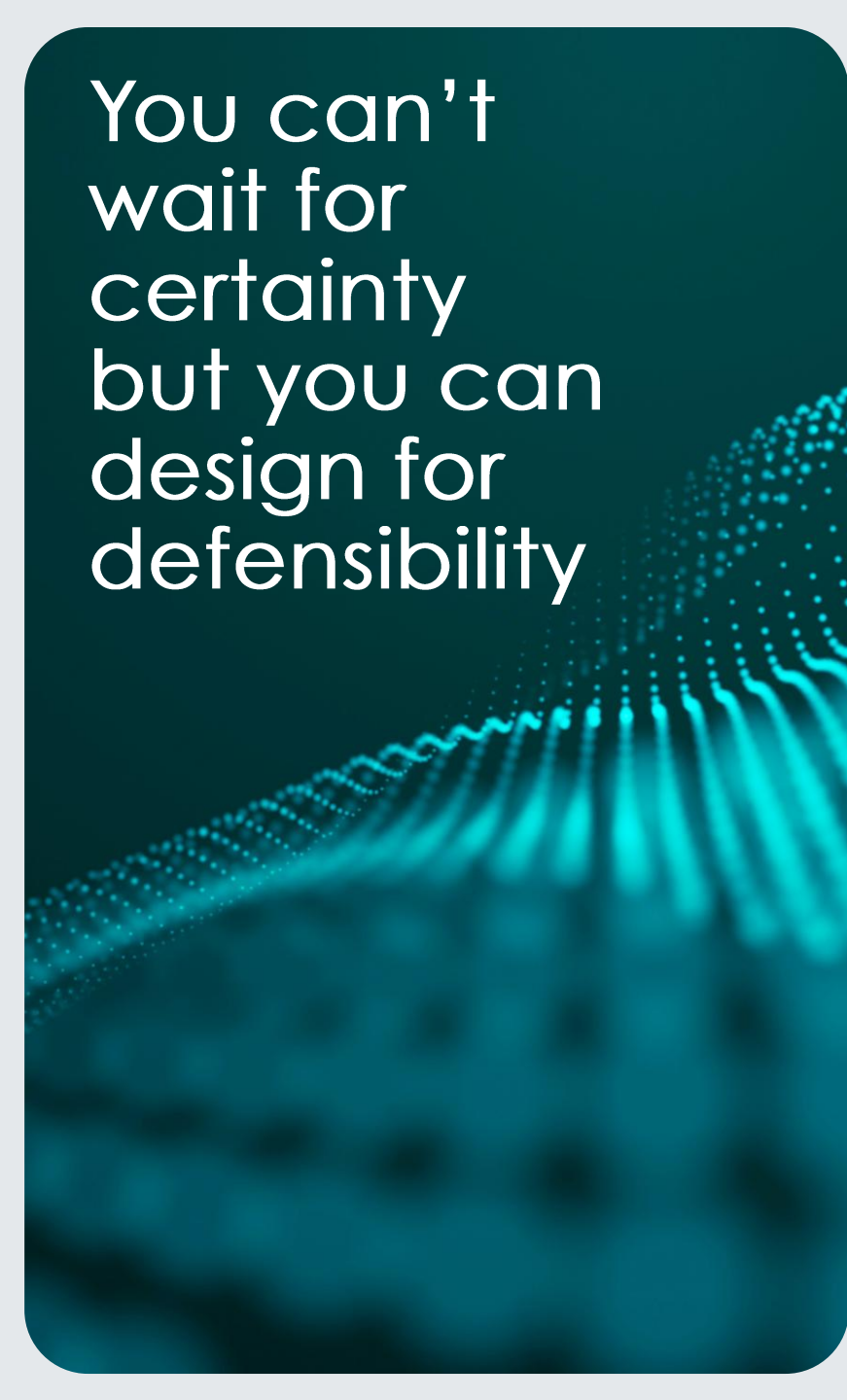
▶ **Ghana** (ethics commentary): Misuse of AI.

# From Risk to Practice

**Judicial direction:** African courts now expect human verification of any AI  
Courts are setting practical precedent AI rules while legislation catches up



**African benches concur:**  
Use AI but verify everything.



You can't  
wait for  
certainty  
but you can  
design for  
defensibility

## Working assumption for business

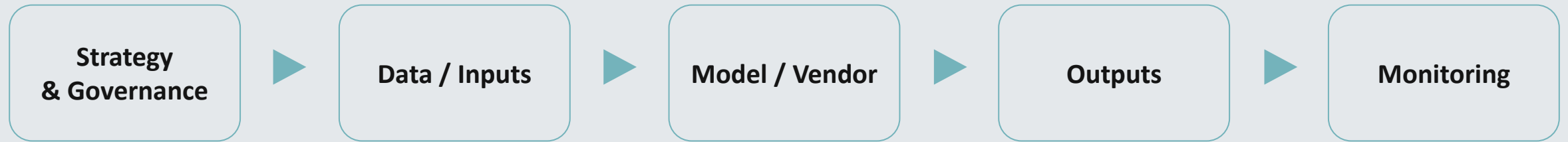
- ▶ Treat AI/IP as an operational governance issue, not a once-off legal opinion
- ▶ Design controls across the lifecycle: **inputs → model/vendor → outputs → monitoring**
- ▶ Document decisions: it's your best protection when the law is unsettled
  - Can AI be used?
  - Which AI tools?
  - What data can be used?
  - Whether outputs can be published?
  - When escalation is required?



# What has changed since the June 2025 conversation?

- ▶ Litigation has moved from ‘is training lawful?’ to ‘prove provenance + manage outputs’
- ▶ Regulation has shifted from ‘coming soon’ to ‘contracting and procurement reality’
- ▶ Boards now expect AI governance, including IP, as part of risk and reporting (King V)

# AI/IP risk sits across the lifecycle



**Readiness** = having controls at each step and evidence they work

# SmartAI IP Readiness Framework (7 categories)

**Strategy & Governance**

**IP Ownership & Protection**

**Data & Training Inputs**

**Outputs & Infringement Risk**

**Confidentiality & Trade Secrets**

**Contracts & Vendor Management**

**Monitoring & Compliance**

# How the Readiness Test works

Fast, structured, and designed for business teams

- ▶ 7 categories | short questions | practical 'evidence-based' answers
- ▶ Produces a readiness snapshot (low → high) and priority actions
- ▶ Designed to trigger the right internal conversations (legal, compliance, IT, product, HR)

**Ad hoc**

**Defined**

**Managed**

**Assured**

# Strategy & Governance

AI/IP risk is now board and audit-visible; governance sets accountability.

## Example questions

- ▶ Do you have an approved AI policy + IP addendum?
- ▶ Is there an AI owner and escalation path?
- ▶ Is AI use reportable to risk/board (King-style governance)?

### LOW readiness

Low: informal use, no owner, no reporting

### HIGH readiness

High: clear policy, owners, board-ready reporting



# IP Ownership & Protection

Know what you own (and can protect) when AI is in the workflow.

## Example questions

- ▶ Do projects log human contribution (authorship/inventorship)?
- ▶ Do you register key marks/watermarks/inventions?
- ▶ Do you manage IP created with vendors/contractors?

### LOW readiness

Low: unclear ownership, scattered assets

### HIGH readiness

High: clear allocation, registration strategy, asset inventory



# Data & Training Inputs

Provenance is the new baseline: licensed, lawful, documented inputs.

## Example questions

- ▶ Do you know what data is used (and under what rights)?
- ▶ Do you check terms, licences, and TDM exceptions?
- ▶ Do you keep an evidence trail + deletion plan?

### LOW readiness

Low: 'we assume it's fine', no logs

### HIGH readiness

High: audited sources, logs, permissions, deletion/exit plan



# Outputs & Infringement Risk

Even if training is arguable, outputs can still create liability and brand harm.

## Example questions

- ▶ Do you have output clearance rules (marketing, product, comms)?
- ▶ Do you prohibit prompts for third-party logos/watermarks?
- ▶ Do you run similarity / trade mark checks for high-value outputs?

### LOW readiness

Low: no or little control

### HIGH readiness

High: clearance searches, FTOs, patentability loops



# Confidentiality & Trade Secrets

AI tools can leak sensitive information; this is often the fastest real-world risk.

## Example questions

- ▶ Is confidential information blocked from public models?
- ▶ Are there approved 'safe' tools (e.g., enterprise environments)?
- ▶ Do NDAs and trade-secret controls cover AI use?

### LOW readiness

Low: staff paste confidential data freely

### HIGH readiness

High: tool controls, training, enforcement



# Contracts & Vendor Management

Your risk often sits in supplier terms: warranties, indemnities, change logs.

## Example questions

- ▶ Do contracts require provenance warranties + indemnities?
- ▶ Do you get model factsheets / disclosures and update notices?
- ▶ Do you have audit + deletion/transition rights?

### LOW readiness

Low: click-wrap only

### HIGH readiness

High: negotiated terms, diligence, change control



# Monitoring & Compliance

**Controls must be monitored:** incident response, audits, metrics, improvement.

## Example questions

- ▶ Do you monitor AI use and outputs in practice?
- ▶ Do you have an incident reporting procedure (IP + data + comms)?
- ▶ Do you track improvements and re-test readiness?

### LOW readiness

Low: no monitoring until crisis

### HIGH readiness

High: metrics, audits, incident drills, continuous improvement



# Interactive (60 seconds)

Pick one: where are you strongest and also, where are you most exposed?

- ▶ A) Inputs / data provenance
- ▶ B) Output clearance / brand risk / FTO
- ▶ C) Confidentiality & trade secrets
- ▶ D) Vendor contracts & warranties
- ▶ E) Monitoring & governance reporting



# From readiness gaps to support

- ▶ We use your results to prioritise: quick wins, policy fixes, contract fixes, and deeper audits
- ▶ Pick the lightest intervention that closes the risk and scales across the organisation

Low on Inputs

- ▶ **Dataset provenance audit + guidance + deletion protocols**

Low in Outputs

- ▶ **Output clearance workflow + brand/trade mark/invention**

Low on Confidentiality

- ▶ **Tool controls + training + safe-use standards**

Low on Contracts

- ▶ **Supplier diligence pack + warranties/indemnities + change logs**

Low on Monitoring

- ▶ **Incident response + periodic re-tests + watch services**

What you'll  
see in 3  
minutes

## Let's do a quick walkthrough

- ▶ How the questions are phrased (business-friendly, evidence-based)
- ▶ How scoring works and what 'good' looks like
- ▶ How to use the output internally: actions, owners, timelines

# Closing: move from uncertainty to readiness the lifecycle

- ▶ Take the SmartAI IP Readiness Test (5–7 minutes)
- ▶ Share the snapshot with your AI, legal, compliance, IT, HR and innovation leads
- ▶ We can help you convert it into an actionable 30/60/90-day plan



[smartaiip.adams.africa](https://smartaiip.adams.africa) | [smartaiip@adams.africa](mailto:smartaiip@adams.africa)

Finally, I  
mentioned  
value  
creation

## AI Risk Controls is really, Intangible Asset Management

### What these controls actually manage

- ▶ Human creativity and judgement
- ▶ Know-how, methods and workflows
- ▶ Business data and refinements
- ▶ Brand expression and goodwill
- ▶ Process and product improvements

### These are unregistered intangible assets:

- ▶ Copyright (unregistered)
- ▶ Trade secrets and confidential information
- ▶ Know-how and improvements
- ▶ Brand goodwill and reputation

### Bottom line

- ▶ Good AI governance protects value, preserves future IP optionality, and converts day-to-day behaviour into enterprise assets.



# crammer<sup>®</sup>

Decoding the Future



Client Survey

# THANK YOU