⇒ LawTech, Tech Law and What's Next

Building the Skills, Infrastructure and Mindset for AI-Enabled Legal Practice

Lisa McClory
lisa.mcclory @cms-cmno.com

AI and Tech-Enabled Legal Practice

AI and technology is increasingly integrated into legal practice:

- Document review
- Summarisation
- Legal research
- Client-facing applications
- Delivering advice and services through portals and platforms
- Cyber risk defence and data governance
- Changes in law and regulation, e.g. digital wills, electronic signatures and deeds

Changing Opportunities – Agile Design and Creativity

Fast-moving technology: new legal-specific models and open AI models

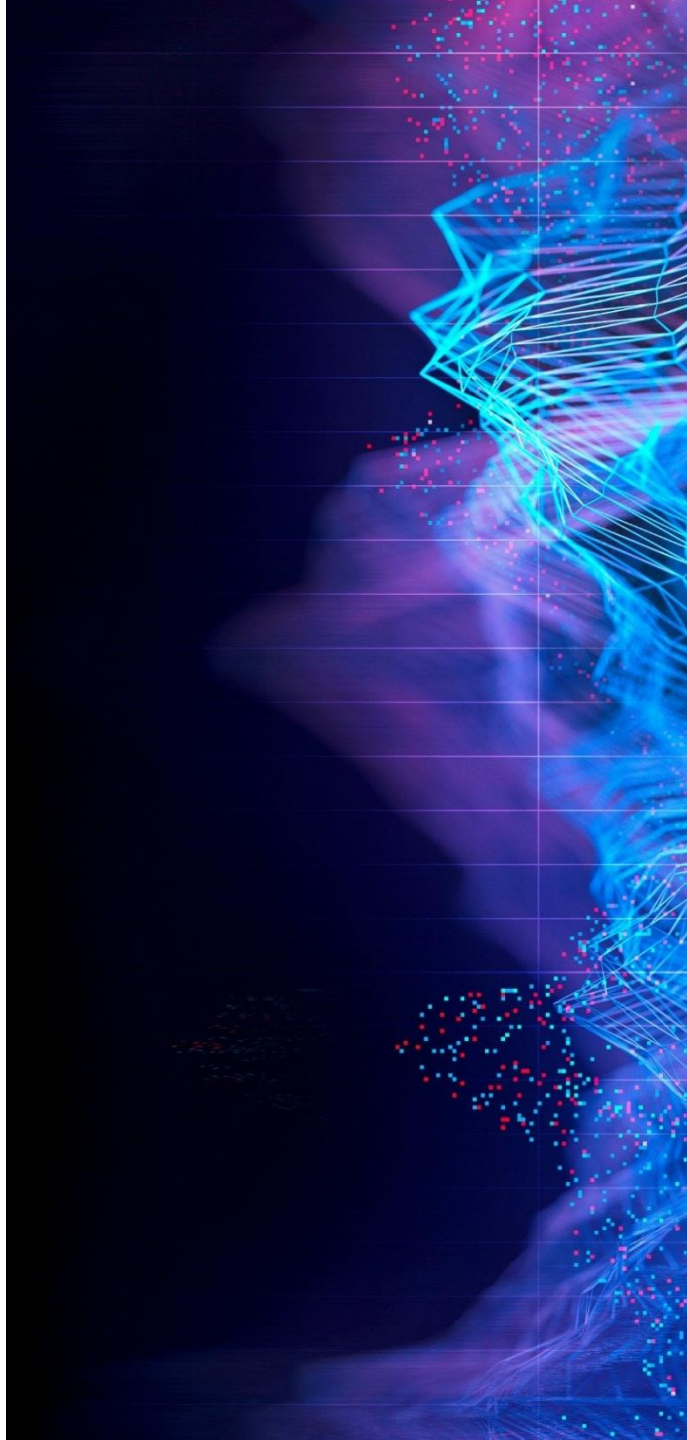
Questions for law firms: do we build own AI system? Lock in to a specific vendor? How and where to invest and what infrastructure is needed?

Focus points:

- GenAI capability
- How to upskill the firm and ensure AI literacy?
- Spreading tools, ideas, innovation: how to plan and scale
- Top down vs grass-roots innovation: individual practitioners creating their own agents?

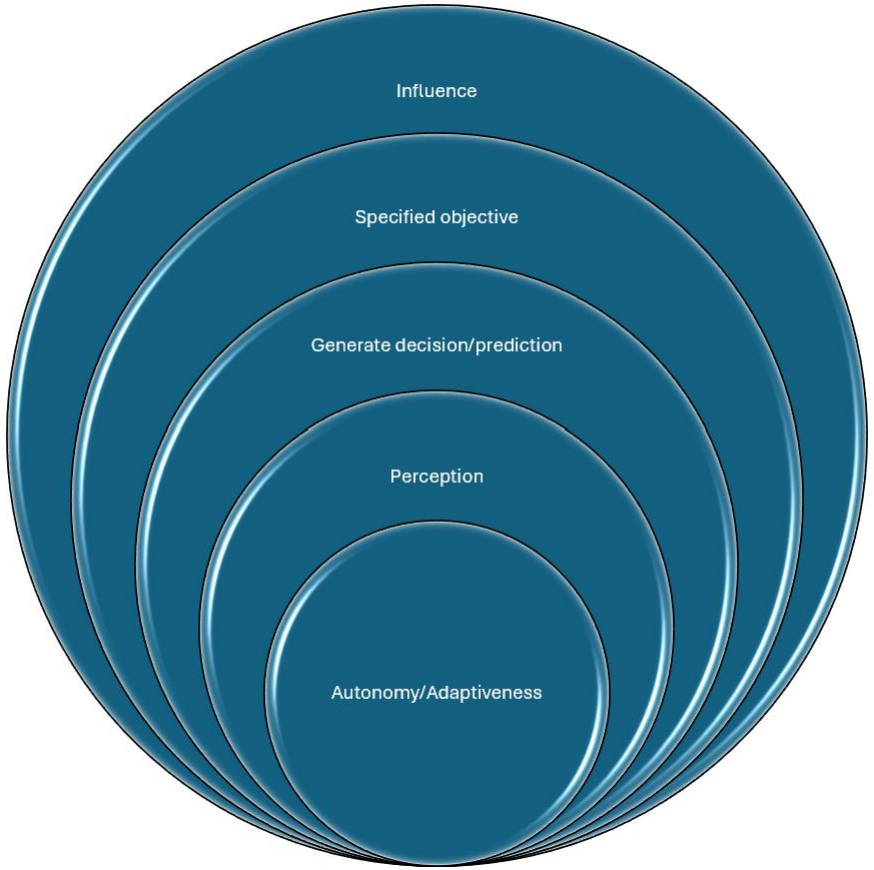
Clients using AI – new touchpoints for lawyers

- AI-enabled legal instructions: receiving prompt outputs
- Clients running legal advice through AI tools: legal privilege?
- Expectations: speed of advice turnaround
- New risks for lawyers: AI oversight – ‘AI burnout’?



AI: what's under the hood and how does it work?

- **AI:** a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments
- **AI model –** connecting to a wider system comprising different technologies:
  - Databases
  - User interface
  - Monitoring and retrieval programs
  - Governance mechanisms



Model and RAG Layer (and MCP Servers)

- **AI model:** the engine that powers the AI system
- **Data orchestration or query layer:** a data model layer that organises databases and directs what data is sent to the model, what kinds of prompts and queries are run and manages token demand
- **RAG (Retrieval Augmented Generation):** a technique enabling a model's response to be grounded in documents retrieved when the model is inferring information – keeps the model tied to a specified corpus of information = better fidelity and reliability and supplements the model's information with proprietary information
- **MCP:** standards of data access running on servers that manage how AI can access data = reduces data risk

- **Agentic AI**

Agentic AI

- Specialised systems that engage in autonomous reasoning to plan, learn and execute complex and multi-dimensional objectives.
- Adopt dynamic planning processing
- Can interact with various tools
- Engage in iterative reasoning

- Additional risks of agentic AI: data control and access; oversight; complexity; transparency; drift and bias: how to implement ongoing governance.

Risks and AI Governance

Risks occur at all levels of an AI system:

- Is the model fit for its purpose?
- Is the AI system equipped with adequate safety and governance features that enable its use in the desired context?
- How has the law firm reached a decision to use this particular system for this purpose, was this made with adequate diligence? What monitoring and governance is in place going forward?
- Does the AI system enable sufficient oversight and transparency?
- Does the firm have the skills and knowledge required to understand, manage and mitigate AI-related risks?

Risk Scanning

Examples of risks:

- Bias: decisions based on unintended inference of private information, including sensitive characteristics such as race and gender, all of which: this could be data that is within the model, combined with information in input prompts;
- Privacy: AI tools may require users to log in and may retain user information. Data can be processed and shared across multiple different actors in an opaque non-transparent way;
- Confidentiality: Confidential information could be added to a prompt, used for model training, causing irretrievable loss of confidentiality. Threads might leak information even without mentioning names
- Fraud risk: AI might be used by malicious actors for fraud or deception, including forgery or impersonation scams; and
- False information: LLM predictions may endorse or spread unethical or harmful views of others.

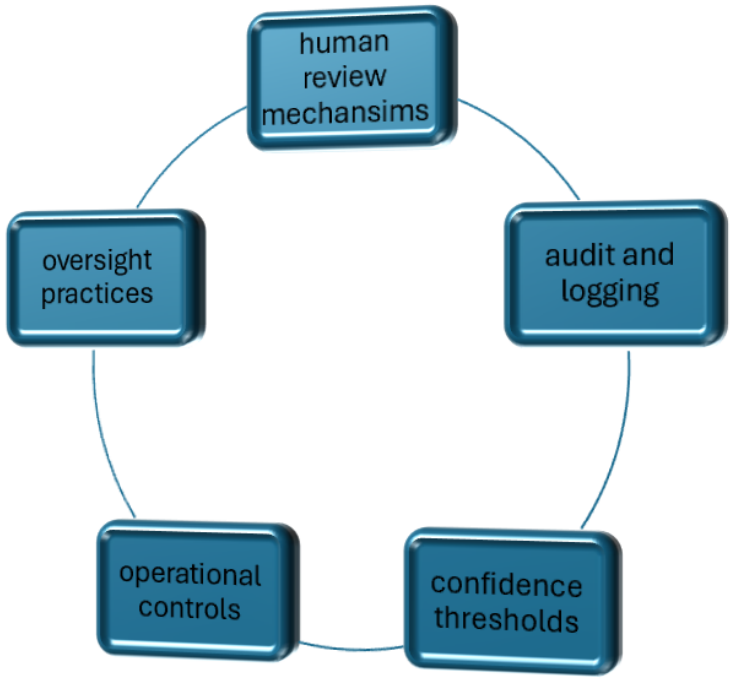
AI Governance Approaches

Governance application to whole system – ongoing

Product and context level governance: multi-layered

What is AI Governance:

(a) whether AI should be used at all;
(b) for what purposes it may be used;
(c) by whom it may be used;
(d) what controls to deploy around AI use;
(e) what form of supervision to be used; and
(f) what the consequences will be if something goes wrong.



Contextual Risks: AI Design

Context-specific risks: e.g. a general-purpose model deployed as a legal advice tool without safeguards / AI model trained on social media data and used as a criminal record or reoffending risk assessment (biases around language styles, political views, etc)

Governance questions to answer:

- who has authority to make decisions?
- what information must they have before making them?
- what risks are acceptable?
- what controls must be in place?
- how are decisions recorded?
- who checks whether the system is working?
- what happens if the system fails?

Simple AI Governance Framework

A simple AI governance framework often includes:

- An inventory of AI systems
- Risk classification
- Policies and accountability
- Data controls
- Human oversight
- Testing and assurance
- Incident management
- Transparency and documentation

Client Best Interests and Professional Duties

Ayinde v London Borough of Haringey, and Al-Haroun v Qatar National Bank

[2025] EWHC 1383 (Admin)

> "The Code of Conduct of the Solicitors Regulation Authority (the SRA) describes the standards of professionalism that the SRA and the public expects of individuals authorised by the SRA to provide legal services. […] Solicitors are under a duty not to mislead the court or others including by omission (Rule 1.4). They are under a duty only to make assertions or put forward statements, representations or submissions to the court or others which are properly arguable (Rule 2.4). They are under a duty not to waste the court's time (Rule 2.6). They are under a duty to draw the court's attention to relevant cases and statutory provisions of which the lawyer is aware and which are likely to have a material effect on the outcome (Rule 2.7). They are under a duty to provide a competent service (Rule 3.2). Further, where work is conducted on a solicitor's behalf by others, the solicitor remains accountable for the work (Rule 3.5)."

Liability for AI Harms

UK Jurisdiction Taskforce Consultation on the Legal Statement on Liability for AI Harms (January 2026)

- ‘Despite the novel and unique qualities of AI, English law is capable of attributing liability to individuals or corporate entities for loss caused by AI. AI does not have legal personality in English law, and so cannot be held liable in its own right.’
- Sources of liability for AI-caused loss:
  - Responsibilities parties have voluntarily taken on;
  - Liability imposed by law regardless of whether a party has chosen to accept that liability.
- It is … possible for a person to suffer physical or economic loss in circumstances where there is no contract, and therefore no contractual counterparty to sue.
- “In practice, the circumstances in which use of AI can give rise to negligence liability for economic harm will generally either involve professional negligence (for example, a financial advisor who negligently relies on AI output to give loss-causing investment advice) or will involve statements made by AI (such as false statements generated by a chatbot).”

Procurement and Responsible Innovation

- **Finding products:** how to get information and engage with vendors: fact-finding and RFI/RFP
- **Launch and testing of new client-facing applications:**
  - Tech partners may release a new feature or collaboration tool
  - Find friendly pilot consultants or clients to test initially, e.g. frictions around user interface, understanding the user's perspective: what is the user's experience?
  - Permissioning: requires particular focus to check data is secured and accessed only as required
  - Important pre-launch – establish clear product governance, test and check and raise questions
- **New ways of working with clients:**
  - Collaborative AI spaces, e.g. shared playbooks, curated workflow agents, shared AI assistant threads (for transactions or knowledge sharing for instance)

Contracting for AI in Legal Practice

- Service Legal Agreement essentials:
  - Usual clauses on availability, support response times and maintenance arrangements;
  - Contractual terms covering whether and how the system can be used in a way compatible with the firm's professional obligations;
  - Boundaries of permitted and prohibited use, including means of data handling, confidentiality, records retention and security guardrails, accuracy of output, auditability, regulatory cooperation
  - Identify the relevant controller, processor or joint-controller relationships, international transfers, data location and retention periods, deletion and export methods and restrictions on uses of personal data
  - Handling of information that is sensitive for privilege requirements
  - Known AI limitations (within SLAs) and change control processes
  - Standards e.g. ISO/IEC 42001:2023 (AI management systems); ISO/IEC 22989:2022 (AI concepts and technology)

Principles of Responsible AI

Practical questions for legal practitioners:

- Is the tool safe and robust enough for this legal task?
- Is it clear when and how AI is being used?
- Could the tool create unfairness or bias?
- Who is accountable for the decision to use it?
- Can an affected client challenge, correct or complain about the outcome?

Scenarios:

- Client AI and Lawyer AI in a Shared Space – what governance applies, where do professional duties become relevant?
- Client perceptions of value: knowledge at marginal cost, lawyers adding judgement
- An AI Agent as a member of your team? AI client-facing agents?

Role of Lawyers and AI

- Role of the lawyer changing emphasis from advice generally on law to assisting clients reaching outcomes and managing risk
- Value of strategic advice, particularly with changing client issues and business models:
  - AI litigation – smart cars, physical AI, profiling and access to products or services;
  - AI use in evidence, e.g. for criminal proceedings and litigation expert reports
- Pricing and value: outcomes-based pricing? New forms of service mediated by AI?
- Ongoing training:
  - Understanding the fundamentals of AI and different types of system, and risks arising;
  - Identifying and understanding how AI is used and risks and key features in legal practice
  - Keeping up to date and fully understanding AI-related risks relevant to legal practice and clients
  - Understanding AI's impact on clients, including clients with characteristics of vulnerability and digital accessibility needs
  - Understanding contractual and professional responsibilities for AI, including data, confidentiality and professional duties, including ethical responsibilities
  - Keeping up to date with AI governance requirements and legal responsibilities