Risks (and safeguards) in the use of AI by IP professionals

John Gray

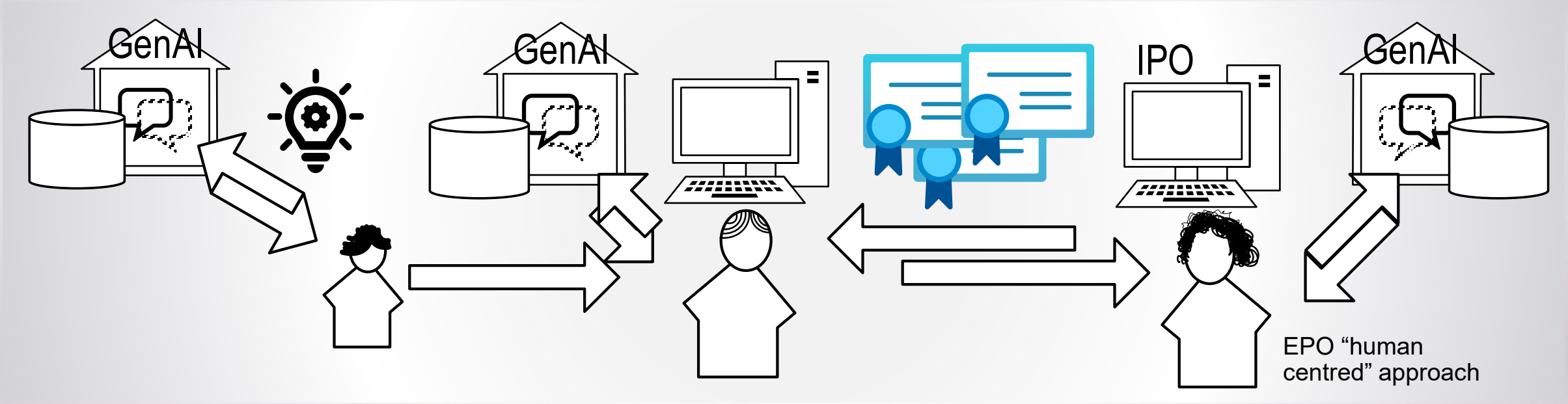
John Gray IP Limited, UK

Disclaimers and apology

The views and opinions expressed in this presentation are those of the author alone and do not necessarily reflect the official position of the **epi** or any other organisation.

The author has not bothered to develop and include glossy AI-generated illustrations for this presentation. More often than not, they look good but fail to illustrate the point accurately.

Generative AI + the “human in the loop”



Quality ↑ Speed ↑ Cost ↓

GenAI has many uses

- Technical Research
  - Prior art searches
  - Landscaping, data analysis
  - Novelty assessment?
- Legal Research
  - Statutes, Rules & guidelines
  - Case Law
- Office automation
  - Practice manuals
  - Costing
  - Portfolio management
  - Minute-taking & summaries

- Drafting help
  - Automate routine tasks
  - Check quality
  - Create text and drawings; claims?
- Prosecution help
  - Analyse prior art
  - Formulate arguments?
- Infringement detection

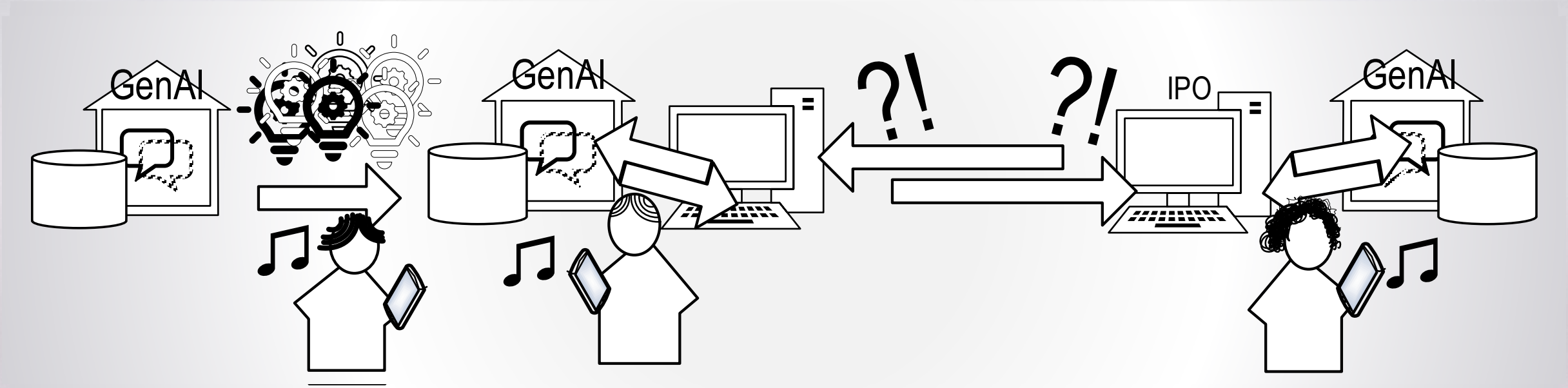
Example chat from EPO legal research tool

Example chat from one AI drafting tool

Limitations of LLMs and Generative AI

- Large language models are trained on vast databases of diverse knowledge, but
  - Does it include **my specialty**?
  - Is it verified as true?
  - Is it kept up to date?
  - Is it biased towards some branches of knowledge?
  - Some types of humans?
  - Does it know about my local laws/culture?
  - Is it trained on illegal/unethical/private materials?
  - …
- The trained model can be used to **predict** the **most likely** output (text/image) from your input text (the "prompt") but
  - The process is **stochastic** (a bit random), not deterministic.
  - Did I include the necessary information/**context**?
  - Is output **contaminated** with copyright/secret information?
  - How can it describe something that is truly new?
  - It can't infer function by looking at a new mechanism.
  - **It will not say "I don't know".** It will do the best it can.
  - **It will make stuff up ('hallucinate'), in the most convincing style.**

Generative AI, “the ~~human~~ in the loop”



How did that happen?
(And who’s to blame?)

Guidelines issued

ABA – First ethics guidance on a lawyer's use of AI tools (Formal Opinion 512)

- Competence
- Confidentiality of Information
- Communications
- Fees

epi – European Patent Attorneys

- epi Guidelines: Use of Generative AI in the Work of Patent Attorneys

The rules of professional conduct are not new *– only the temptations and risks are new*

IPREG – UK patent and trade mark attorneys

- Interim guidance

CIPA – Chartered Institute of Patent Attorneys (UK)

- AI guidance for SMEs and creators – Advice for inventors and clients.

CITMA - Chartered Institute of Trade Mark Attorneys (UK)

- Choosing your AI tools & vendors: Top 5 tips for trust and partnership assessment:
- The "trust equation": Credibility, Reliability, Sector familiarity, User-focused

CNIPA – Chinese State IP Office

- Warnings to both professionals and applicants

Competence – the attorney is <u>always</u> responsible

epi: "*Members remain **at all times responsible** for their professional work, and cannot cite the use of generative AI as any excuse for errors or omissions. …Members **must check any work product** produced using generative AI for errors and omissions. ..*"

- Ask for sources, but **check don't trust**.
  - Verify every reference exists AND says what the AI says it says.
    - Use further prompts to test the first answer. Either with the same AI or a competing/supervising one.
      - e.g. "*<u>Where</u> in D1 does it describe an example with features A and B combined?*"
    - Find better tools, either GenAI or more conventional automation.

What's the point of the AI if I have to check everything? ("Truth Tax")

Confidentiality – do not trust, verify

epi: "***If there is doubt*** *that confidentiality will be maintained to a level that is appropriate to the prevailing context* ***the AI model in question should not be used****…. **Members must inform themselves** about the likelihoods and modes of non-confidential disclosures deriving from use of specific AI models.*"

IPREG: "*You have a* ***fundamental duty to safeguard your client's sensitive information****. If you intend to use AI,* ***you must understand*** *whether and how any information provided when using the product will be stored and secured. ..*"

Some things are more sensitive than others.

Beware - ‘FREE’ AI will train on your data

“*If you are not paying for the product, you <u>are</u> the product*”

Or are you paying for it with your <u>client’s</u> trade secrets?

Patents:

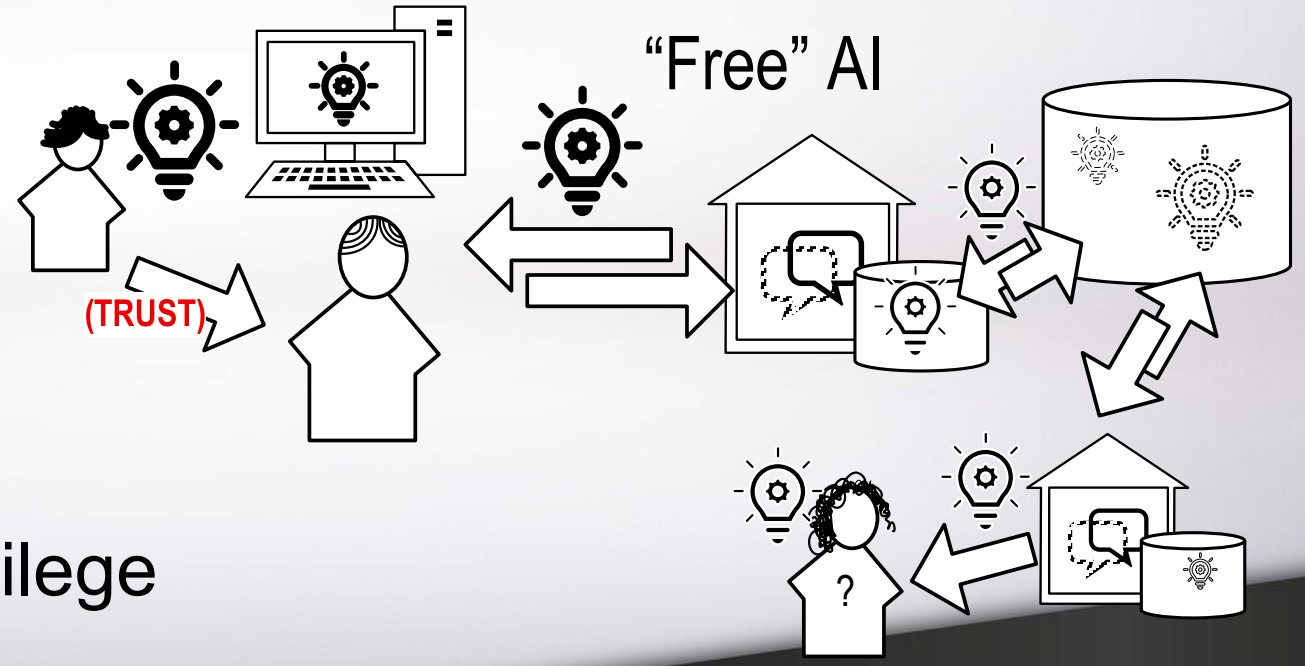
- Novelty destroyed by non-confidential disclosure.

Commercial secrets:

- Could leak

Advice:

- Loss of attorney-client privilege



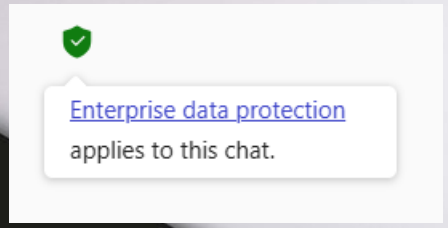
Confidentiality: Cloud solution OK?

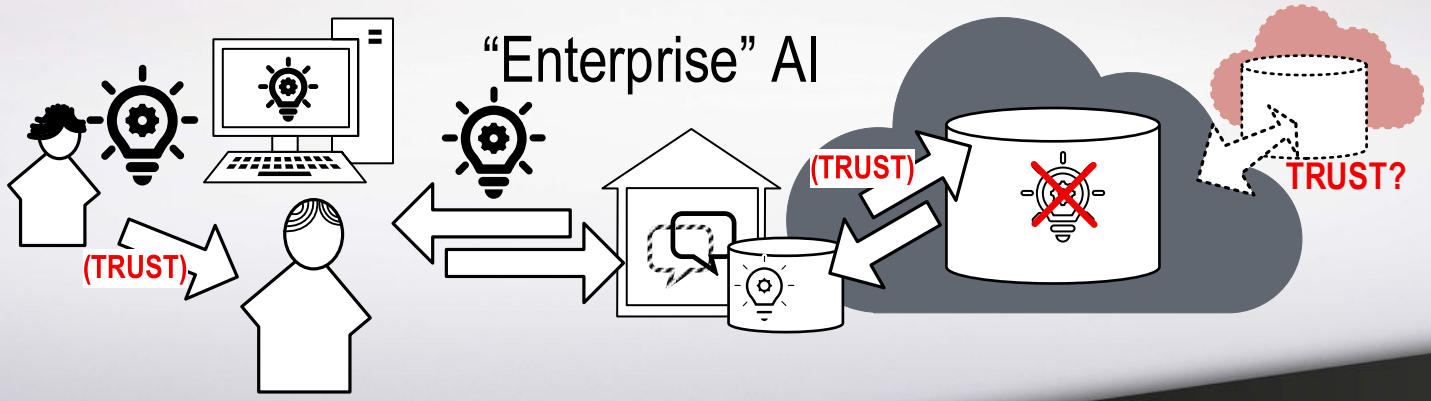
Secrets are safe, by everyday standards…

- Confidential by contract/law
- No training the AI on your data
  - → Patent novelty assured
  - → Privilege OK
- Familiarity "everyone uses the Cloud"
- Modest expense and infrastructure

…but they are on *someone else's computer*…

- Where is my data? EU? US? (residency)
- Who do you send it to behind the scenes?
- How long do you keep it? (retention)
- How secure is it against spying?
- What if your company goes bust?

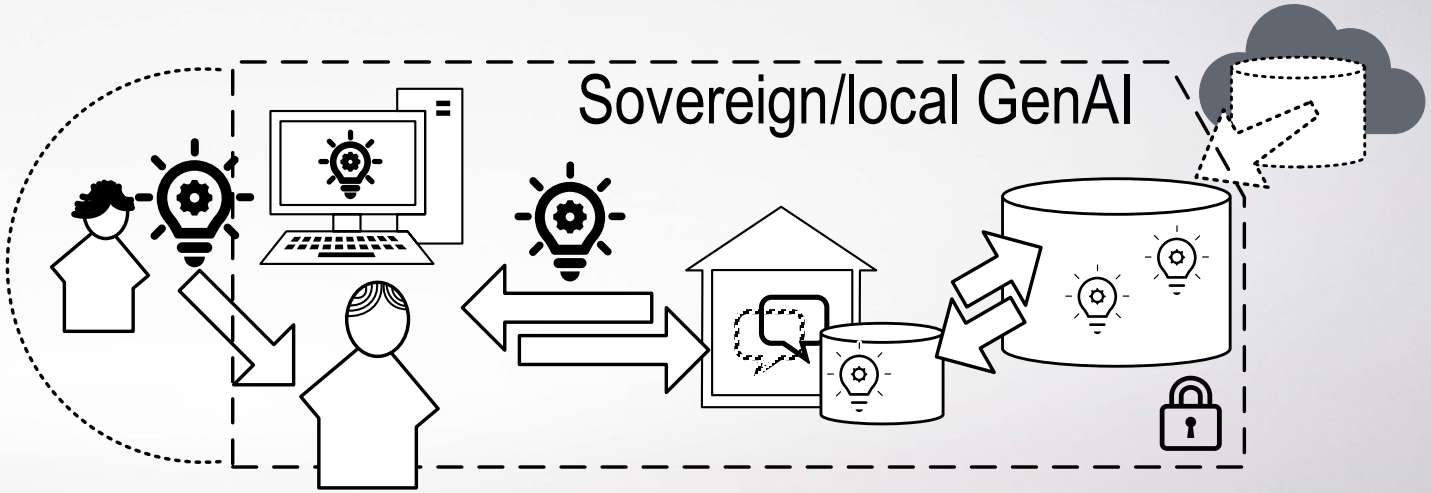




Confidentiality: ‘sovereign’/local AI

Secrets are safe, by your chosen standards

- Confidential by contract/law
- No training *other people’s models* on your data
  - → Patent novelty OK
  - → Privilege OK
- Custom train *your own models*
- Secure: secrets never leave your premises



But… you’re gonna need a bigger computer!

Communication/transparency

epi: "*Members **must** in **all** instances establish, **in advance** of using generative AI in their cases, **the wishes of their clients** with regard to the use of generative AI*. …"

- Do these wishes match the capability of your preferred AI tool?
- Do you need different tools/settings/accounts for different clients?

*"Members are **not** required to state, **in communications with the European Patent Office** and Unified Patent Court, that generative AI has been used in the production of work, unless …"*

Some clients are more sensitive than others. But **the attorney still bears the ultimate responsibility** for professional standards.

Fees/charging

- **IPREG**: "*There is **no requirement to pass on costs savings achieved by the use of AI to the client** as how you choose to bill for your work is a matter for you. **However**, you should bear in mind your **overarching duties to act in your client's best interests** and to provide **transparency** about billing.*"

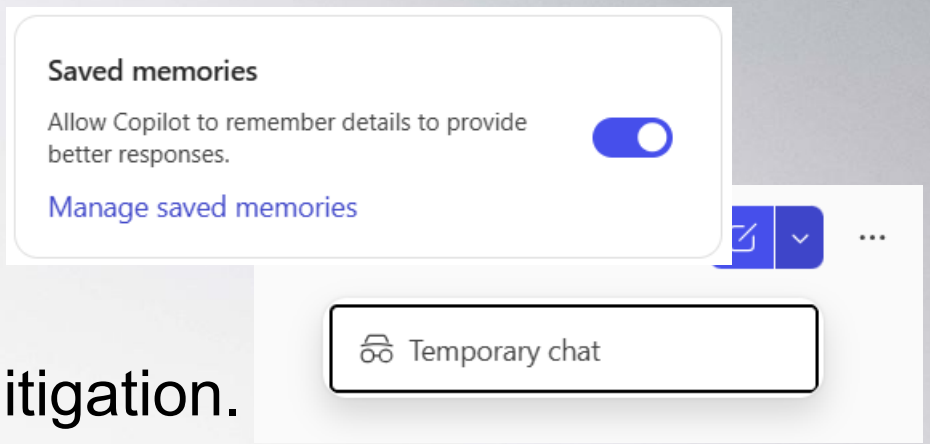
- **ABA**: "…*if a lawyer uses a GAI tool to draft a pleading and expends 15 minutes to input the relevant information into the program, **the lawyer may charge for that time as well as for the time necessary to review** the resulting draft for accuracy and completeness. But, **in most circumstances, the lawyer cannot charge a client for learning how to work a GAI tool.***

Hidden/long-term risks 1

- How much time do you spend checking the AI output – is it cost-effective? When will it be cost-effective? (Can I improve my prompting?)
- Will clients take the same care over confidentiality?
- Will clients no longer see the value of our expertise? Will they just choose vendors using AI to draft a patent at low cost?
- CIPA AI guidance for SMEs and creators:

"The patent system fundamentally relies on human invention and absolute confidentiality before filing. AI tools, whilst offering efficiency gains, threaten both foundations. A single confidentiality breach or over-reliance on AI-generated content could render years of R&D worthless. The true cost of AI errors may only emerge during litigation or licensing negotiations years later."

Hidden/long-term risks 2



- AI's "opinions" on file may have to disclosed in litigation.
- **Skills/recruitment/demographics** – How to pass on/acquire the familiar professional skills in a new working environment? Who gets left behind?
- **"Feature creep"** – AI creeps into our conventional tools & could be used unconsciously: MS Copilot, Gemini, Meta AI colonising and submerging regular apps; plugins like Grammarly; Zoom AI Companion
  - Do these AI functions have to be disabled/re-approved with clients?
  - Will my AI respect confidentiality between clients?
- Are new recruits addicted to using GenAI for everything?

How to begin? – Play safe, but play & learn!

Experiment & learn different tools

- Use opportunities to get familiar with GenAI in routine work (non-confidential)
- Who learns first? How/when does whole firm learn? (Do they want to?)

Choose the right tool for the job.

- General purpose vs Special purpose:
  - Which general-purpose tool is best for task X?
  - Which special purpose tools have added value?
- **GenAI can't do everything**. It can be safer to use old-fashioned automation – deterministic vs stochastic.
  - But you can use GenAI to help design your automation!
- Don't expect a patent at the press of a button. **Supervise and challenge the AI.** Ask it **to challenge your own work.** Ask it to **defend its own work.**

CITMA guidance – Choosing your AI tools & vendors:

Top 5 tips for trust and partnership assessment:

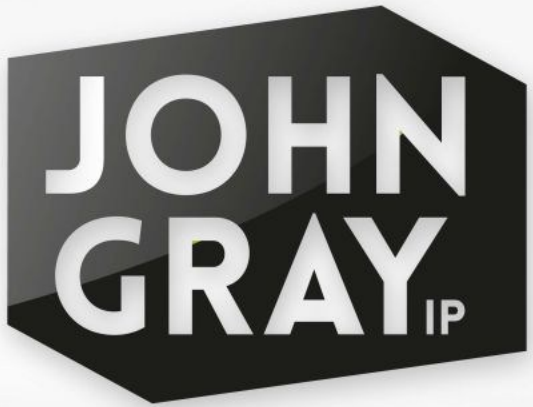
- The “trust equation”:
  - Credibility,
  - Reliability,
  - Sector familiarity,
  - User-focused
- Verify data privacy, confidentiality, and isolation standards
- Require evidence of transparent governance and oversight

Further reading/training

Blogs and podcasts, training

- Bastian Best Software Patent Attorney
- IP Lawyer Tools by Martin Schweiger: section “Robot Patent Drafting”
- Russell IP - IP Tool Demo Day: Exploring Nine IP Tools
- EPO podcast Exploring AI in the patent profession
- *Insight **epi*** podcast
  - epi guidelines: Use of generative AI
  - AI in patent practice: A reality check
  - AI at the EPO: Learning from the best -
- IPKat articles on AI
- Responsible AI UK Rai UK – Research on ethics and regulation

Discuss …



John Gray IP Limited | The Vital Spark®
SC486291 | Regulated by IPReg | 07860 945348 | +44 7860 945348