Sheppard

Top 10 Overlooked Legal Issues with AI

Presented to ACC – So Cal.

April 16, 2026

Jim Gatto
AI, Robotics and Quantum Team Leader | **Sheppard**
jgatto@sheppardmullin.com
703-989-9288

Speaker Biography

James Gatto

J.D., Georgetown University Law Center, 1988

B.E., Electrical Engineering (Physics minor), Manhattan College, 1984

Former U.S. Patent Examiner

jgatto@sheppard.com

703-989-9288

Bio

I am passionate about the intersection of disruptive tech, law and business

38 years of business-focused, legal advice on all aspects of intellectual property strategy, technology transactions, technology-related regulatory issues and litigation, especially ones driven by new business models and/or disruptive technology.

AI, Robotics and Quantum Team Leader

- **Artificial intelligence** (training, policies, IP, regulatory) 26 years
- **Quantum Technology and Robotics** (IP, regulatory, compliance) 15 years
- **Open Source** (audits, diligence, license issues, policies) 28 years
- **Blockchain** (blockchain games, crypto/NFTs, metaverses, digital art) 14 years

Some Recent AI Activity

- Adjunct Professor, George Mason Law School “Emerging AI Legal Issues”
- Adjunct Professor, Ole Miss Law School “Legal Issues with AI”
- Invited Speaker, Korean Copyright Office “AI and Open Source”
- Speaker, US Copyright Office Listening Session on AI Authorship
- Speaker, USPTO Listening Session on AI Inventorship Issues
- ABA-IPL AI/Machine Learning (AI/ML) Task Force
- Member, Artificial Intelligence Committee, International Technology Law Association

Sheppard

Overview of Topics to Cover

1. Applicability of “AI laws” to non “AI tools” and “Non-AI Laws” to “AI Tools”
2. Public Data and Training AI
3. Limitations on Using Your Own Data to Train AI
4. Legal Complications with AI Recorders and Note Takers
5. Legal Complications of AI Code Generators
6. Who is liable for infringing output of AI Tools?
7. Are you indemnified for infringing output of AI Tools?
8. IP Protection for AI Outputs
9.. Ownership of AI output
10. What’s Needed for an Effective AI Governance Policy

Bonus!

1. “AI laws”/ “AI tools”

Applicability of "AI laws" to non "AI tools" and "Non-AI Laws" to "AI Tools"

- There is no standard definition of AI - **It's not just Generative AI**
- **AI Tools – Tools with AI**
- **Overly broad AI definition may cover Non-AI tools**:
  "an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments." CA ***A.B. 2885*** (2024)
- **Some do not reference AI but are broad enough to cover it:**
  "automated employment decision tool" (AEDT). Doesn't mention AI but covers AI tools that assist with employment decisions
- **Free Tools – Enterprise Tools**

Takeaway: Beware of labels – dig into facts

Sheppard

2. “Public” Data Issues

Training Data

A common misperception is that publicly available information is free to use for AI training. Various limitations may apply:

License Terms/TOS

Nature of the Data

Technical measures on site

Manner of acquisition may present issues (e.g., scraping)

License/ToS

Public data is often subject to license or ToS that limit uses or impose conditions

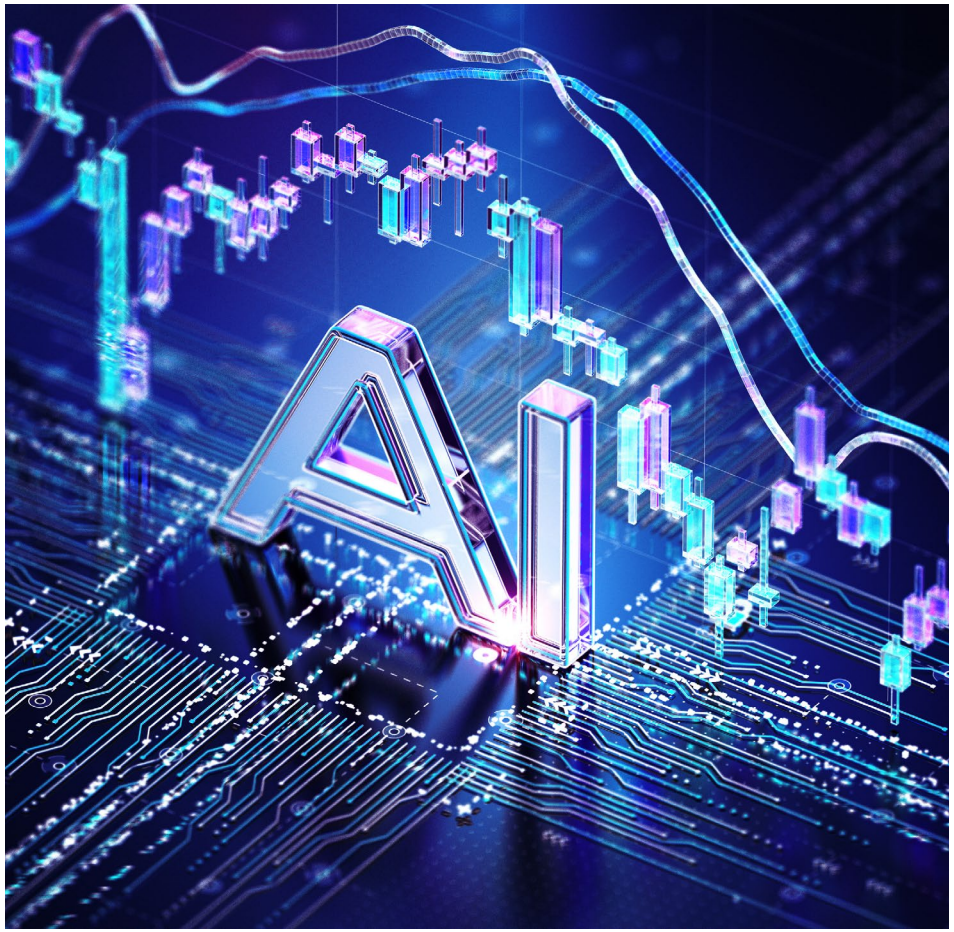
- No commercial use
- No training AI
- Share-alike provisions

Training Data – Copyright

- **Copyright infringement**: using protected text, images, video, music, code, or other works without permission to train a model
  - 100 lawsuits on use of copyright to train AI – infringement or **fair use**
  - 3 key decisions – 1 infringement (*Thomson Reuter*); 2 fair use (*Bartz*, ***Kadrey***)
  - Manner of acquisition matters – for works obtained from “shadow libraries” fair use found not applicable

Training Data – Protected Data

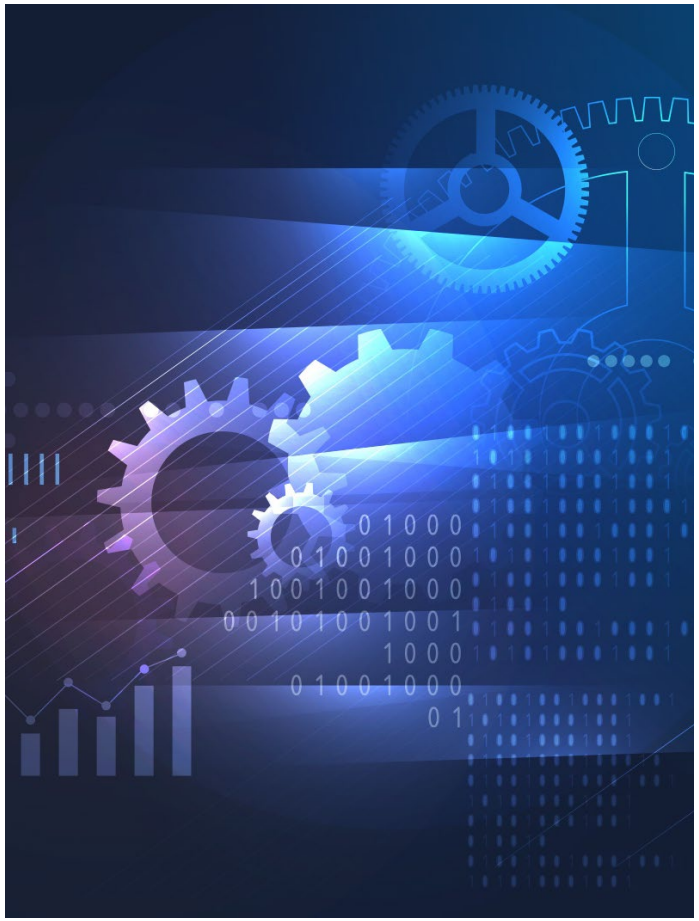
- **Privacy**: collecting or using personal data from public websites in ways that allegedly violate privacy laws or expectations
- **Biometrics**: using publicly available photos, face, voice data without the notice or consent required by state biometric laws
  - Growing number of lawsuits on NIL issues, voice cloning
- **Unfair competition/consumer protection**: based on claims that the data was used or obtained deceptively, or that users were not properly informed (e.g., Cal. Bus. & Prof. Code § 17200)



Training Data – Trade Secret/Databases

If the data collection reaches beyond public information or violates database protections - may be actionable

- Even a database including **public data may be a trade secret** – compilations (e.g., databases) may qualify as trade secrets if the selection and/or arrangement of the data derives value from secrecy.
- *Compulife Software, Inc. v. Newman*, et. al., No. 21-14074 (11th Cir. Aug. 1, 2024), publicly available insurance quotes lack trade secret status, but confidential rate database upon which the quotes are generated can be a trade secret; bots accessing the database improperly was a trade secret violation.



Sheppard

Training Data – Technical Measures

Cannot circumvent technical measures to access data

- Passwords
- Paywalls
- Anti-bot technology
- Other

Growing number of lawsuits focus on:

Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. §1030

Digital Millennium Copyright Act (“DMCA”) 17 U.S.C. §1201

Training Data – Manner of Acquisition

Even without circumvention of technical measures, how you access the data may create legal issues

- Web scraping
- Creating fake/multiple accounts

3. Limitations on Using Your Own Data to Train AI

Limitations on Using "Your" Data to Train AI

1. Need to *acquire* data properly
2. Even if properly acquired (e.g., customer data) you need the *right to use* the data for training AI (*heightened concerns with protected data – PII, Biometrics, COPPA)*

Just Because It's "Your" Data ≠ Right To Use

- Many companies have troves of valuable user data and naturally want to use it to train or fine tune AI
- Use of customer data that exceeds use permitted by the privacy policy/terms in effect at the time the data was collected may be problematic

Legal Considerations When Using Consumer Data To Train AI

- Merely changing TOS/PP to permit use of previously collected data may not work

FTC Warns About Changing Terms of Service or Privacy Policy to Train AI on Previously Collected Data

Sheppard

FTC Settlement- Severe Penalty!

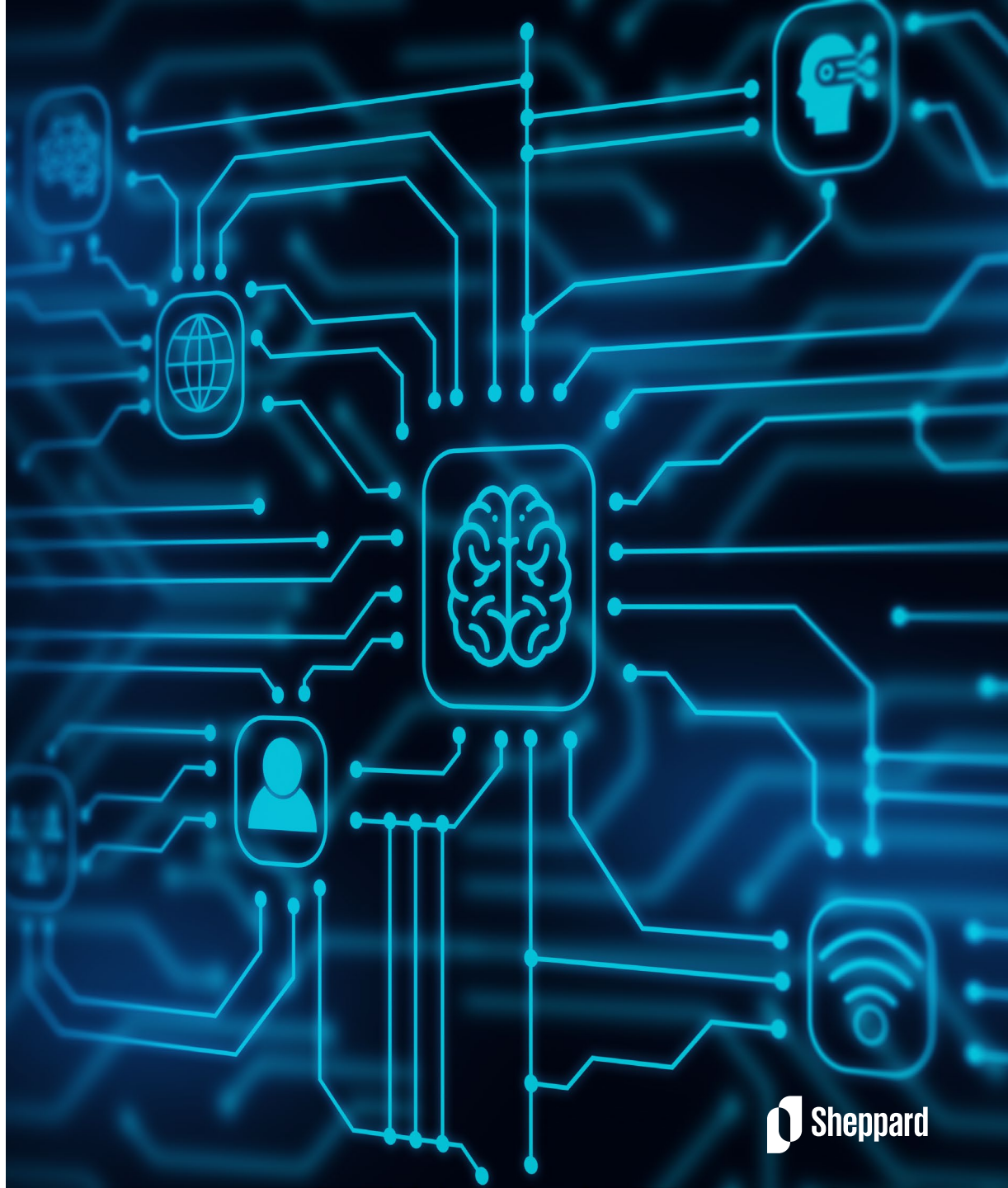
- *Everalbum* – 2022 FTC enforcement for unauthorized use of images **properly collected** for one purpose (online photo service) but used for another (training facial recognition tool)
- Result: "Algorithmic disgorgement"
- Severe penalty for improperly using data to build algorithmic systems (e.g., AI/ML models)
- Required to destroy models/algorithms derived from improperly used data
- *Takeaway*: don't risk loss of investment in training due to improper collection or use of training data

Sheppard

Sample Tool-Specific Legal Issues

Tool-Specific Issues

- Most AI policies are broad and focus on GenAI tools (e.g., creating text, images, video, music, etc.)
- This is necessary, but not sufficient!
- Some “AI tools” create unique issues. Each must be:
  - i) evaluated separately for the business, legal and **ethical** risks they present; and
  - ii) addressed as part of your AI policy



4. AI Note Takers and Recorders

AI Notetakers and Recorders

- **Many "free" tools are dangerous, yet users have no idea of the issues! Creates legal/business risks**
- **Lawyer use of these tools implicates ethical considerations!**
- Vendor diligence – must understand how tools work and features (for approving tools and **ethical** obligations)
- **many tech teams not trained on spotting legal/ethical issues – legal diligence is necessary**
- Develop policies on use of AI notetakers and recording – only permit use of approved tools in accordance with policy

"Listen Up" if Your AI Policy Does Not Cover AI Recording Issues

Growing number of litigations against tool providers and some **users**

AI Notetakers and Recorders Litigation Update

Sheppard

Summary of Issues

1. Understanding operation and features
2. Transparency, Notice and Consent
3. Handling Participants That Do not Consent
4. Applicability of Wire Tapping/Privacy Laws
5. Review for Accuracy
6. Confidentiality and Privilege – Storage and Access Control
7. Retention and Deletion Policies
8. Vendor Diligence
9. Update AI Policies to Include Use of AI Notetakers

Sheppard

Understand Differences in Operation

- Scope of functions – record, transcript, summary, to-dos, *sentiment analysis (*often implicates biometrics/heightened protection*)*
- Notice and consent management – often illegal to record without
- Handling participants that do not consent
- What happens with outputs?
  - Host only, all participants, **tool provider?**
  - Stored – if so, where? Who has access?
- These are business records and subject to discovery - integrate AI policy with document retention and deletion polices

Sheppard

Sample Laws

- Federal Wire Tapping Law
  - 18 U.S. Code § 2511 – Interception and disclosure of wire, oral, or electronic communications prohibited (subject to exceptions)
- State laws
  - CA Penal Code Section 631(a)) imposes civil and criminal *liability on individuals that aid and abet third parties* who secretly eavesdrop on communications or intentionally intercept communications without obtaining consent
  - If you hire a third-party service who uses output without the appropriate precautions, you may be **liable for aiding and abetting**

Sample Ethical Issues with AI Notetakers

Lawyer use of AI notetakers **or participation on calls where used** may implicate ethical considerations

Sample Issues:

- Lawyers have ethical obligation to understand the technology and review for accuracy (ABA MRPC 1.1 - Duty of Competence)
- Must Protect Privilege – who gets a copy? Tool provider? (ABA MRPC Rule 1.6 – Confidentiality)
- Lawyers misuse/nondisclosure of AI recordings may be unethical (ABA MRPC 8.4 - Misconduct)
- Must supervise/train staff on use of these tools (ABA MRPC 5.1 - Duty to supervise)
- If client wants to record – inform client of risks of loss of confidentiality and privilege (MRPC 1.6)

NYC Bar Guidance Formal Opinion 2025-6 (AI notetakers);

A Third Court Addresses AI Privilege and Protective Order (AI and Privilege generally)

Sheppard

Heartland Dental, LLC and RingCentral, Inc.

- The putative class action was filed against Heartland Dental, LLC ("Heartland") for using a third-party AI service provided by Ring.
- Ring was not a party to the calls yet listens to and analyzes phones calls in real time using its AI tool without notice to the dental patients.
- Features include (i) real-time voice transcription, (ii) call highlights, (iii) automated call summaries and (iv) *sentiment* voice analysis.
- Alleged violation of the Federal Wiretap Act. 18 U.S.C. § 2510 *et seq.* and particularly, 18 U.S.C. § 2511. It primarily deals with the interception and disclosure of wire, oral, or electronic communications.

For more see here.

AI Generated Sentiment Analysis/ Emotion Detection

- Emotional AI (sentiment analysis/emotion detection) often processes biometric data (e.g., facial expressions, voice tone, physiological signals), which can be considered **sensitive personal data** under laws like the EU GDPR, California Consumer Privacy Act (CCPA), BIPA, among others.
- Be aware when tools include these functions, ensure compliance and address this in AI Policy

- Takeaway: Other AI tools present other legal issues – each type needs to be assessed and addressed in AI policy

Sheppard

5. AI Code Generators

AI Code Generators

- Most developers are using these tools - some estimates that over 80% of code is AI generated
- Most tools are trained at least in part on open source (OS) software
- If outputs OS code, may "taint" your proprietary software
- **Developers typically do not know when output is OS or what license governs its use**
- Some tools have risk mitigation tools (e.g., filters, reference)
- At least one lawsuit on removal of CMI relates to AI code generators
- Must update OS policies to address use of these tools

Takeaways:

- **Diligence and approve AI code generators based on risk mitigation features**
- **Update OS policies to address use of AI code generators**

Solving Open Source Problems with AI Code Generators – Legal Issues and Solutions

Removal of Copyright Management Information

- DMCA 1202 – liability for removal of CMI or publishing content with CMI removed (scienter requirement)
- CMI removal may not require infringement
- Courts are split on applicability – recent oral argument at Ninth Circuit
- Keep an eye on this decision

6. Who is Liable for Output of AI Tools?

Output Liability Issues

- Liability may arise if output:
  - Infringes IP
  - Includes copyrighted content w/o CMI (DMCA)
  - Contains PII, biometrics, NIL
  - Is defamatory, false or inaccurate
  - Biased or discriminatory
  - Others

Sheppard

Output Liability Issues

Who is liable for bad outputs?

Walters v. Open AI – false output led to defamation claim – dismissed on SJ

If output infringes copyright, who is liable – tool providers or users?

- ***Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984)** – If a device is sold for a legitimate purpose and has a *substantial non-infringing use*, its manufacturer will not be liable under copyright law for potential infringement by its users.

7. Who Indemnifies Who with AI?

Indemnity Provisions with AI Tools

- Many “free” tools pin liability on user and require **user to indemnify the tool provider**!
- Some tools (mostly “paid/enterprise” versions) provide indemnity…but
  - note limitations
  - some impose **obligations or preconditions on you for the indemnity to apply**
- Most lawsuits to date have been against tool providers but suits against users are inevitable

Sample Indemnity Issue

Free versions –

Microsoft does not make any warranty or representation of any kind that any material created by the Online Services does not infringe …

You agree to indemnify and hold harmless Microsoft … arising from or relating to your use of the Online Services, including **your subsequent use of any content** from the Online Services

Copilot Copyright Commitment

Exception: Covers potential infringement by use of output of Microsoft's Copilots and Azure OpenAI Service for paid versions of Microsoft commercial Copilot services, Bing Chat Enterprise, Microsoft 365 Copilot and GitHub Copilot.

- Must implement required "guardrails and mitigations" to be eligible (many companies are not aware of these preconditions!)
- If a customer tenders a claim for defense, the customer will be required to first demonstrate compliance with all relevant requirements

Takeaways:

- **Diligence on tools should assess liability/indemnity terms**
- **Only approve tools where you have indemnity**
- **Comply with and document any preconditions for indemnity to apply**

Sheppard

8. IP Protection for AI Outputs

US Copyright Office Guidance

- Published guidance on registering works that contain material generated by AI:
  - **No AI Authors** – copyright can protect only material that is the product of human creativity - human had **creative control** over the work's expression and "actually formed" the traditional elements of authorship – **prompts usually not enough**!
    - AI generated work itself typically is not protectable
    - Can protect work that uses AI elements where a human selects and arranges (e.g., compilation) and still protect
  - **Disclosure Requirements**: duty to **disclose** and **disclaim** the inclusion of AI-generated content in new, pending and issued copyright registrations

Takeaways:

- **Be careful using generative AI to create content that you want to protect via copyright – some AI policies preclude this use case**
- **If you have registrations that used AI content – need to do supplemental registration**

Patentability of AI – Generated Inventions

AI is not a person and cannot be listed as an inventor

Initial guidance – focused on test for joint inventorship

Revised Guidance – rescinded initial guidance and focused on human conception

Key is whether a person conceived the invention under the traditional conception standard

AI as a tool can assist inventor but human must be the one who **conceives** the invention

Human must contribute more than just operating or interpreting AI output; they must be the source of the inventive idea

Takeaways:

- **Many companies are requiring documentation of human contribution to establish human inventorship**

9. Ownership of AI Output

GenAI Output Issues

- Whether outputs are confidential depends on the terms and features of tools
- Some grant ownership to user, some don't, some don't address
- Some require **license grant to tool provider**
- Many "free" tools pose these risks; "enterprise" version often avoids these issues
- But even with enterprise - some recognize another user's prompt may generate same output and **they own it too**

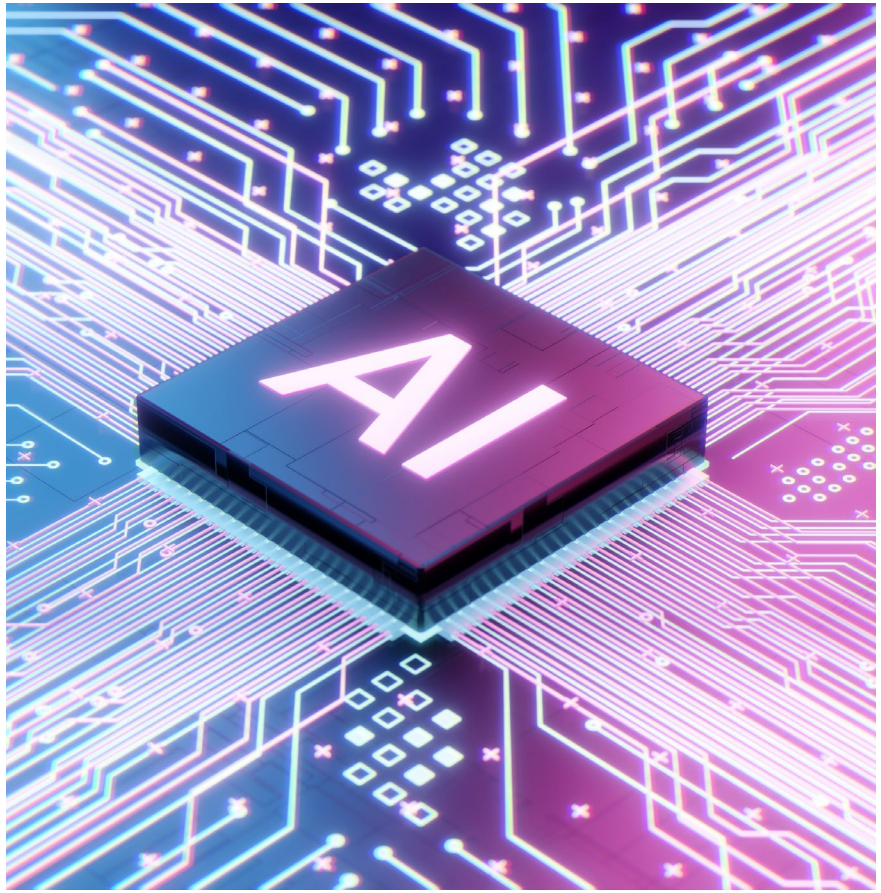
10. Effective AI Use Policies

AI Policies

Sheppard

Overview of AI Policies

- Companies need policies to manage AI legal risks
- Companies need to develop an AI governance committee with representative stakeholders
- Companies need to understand the legal issues and business ramifications to develop effective policies
- Policies need to be “role-based” depending on company’s interaction with and uses of AI
- Inventory tools/use cases – consider unique issues
- Policy should be rolled out with employee training – should be mandatory
- Policies need to be updated regularly
- Company forms/agreements should address AI



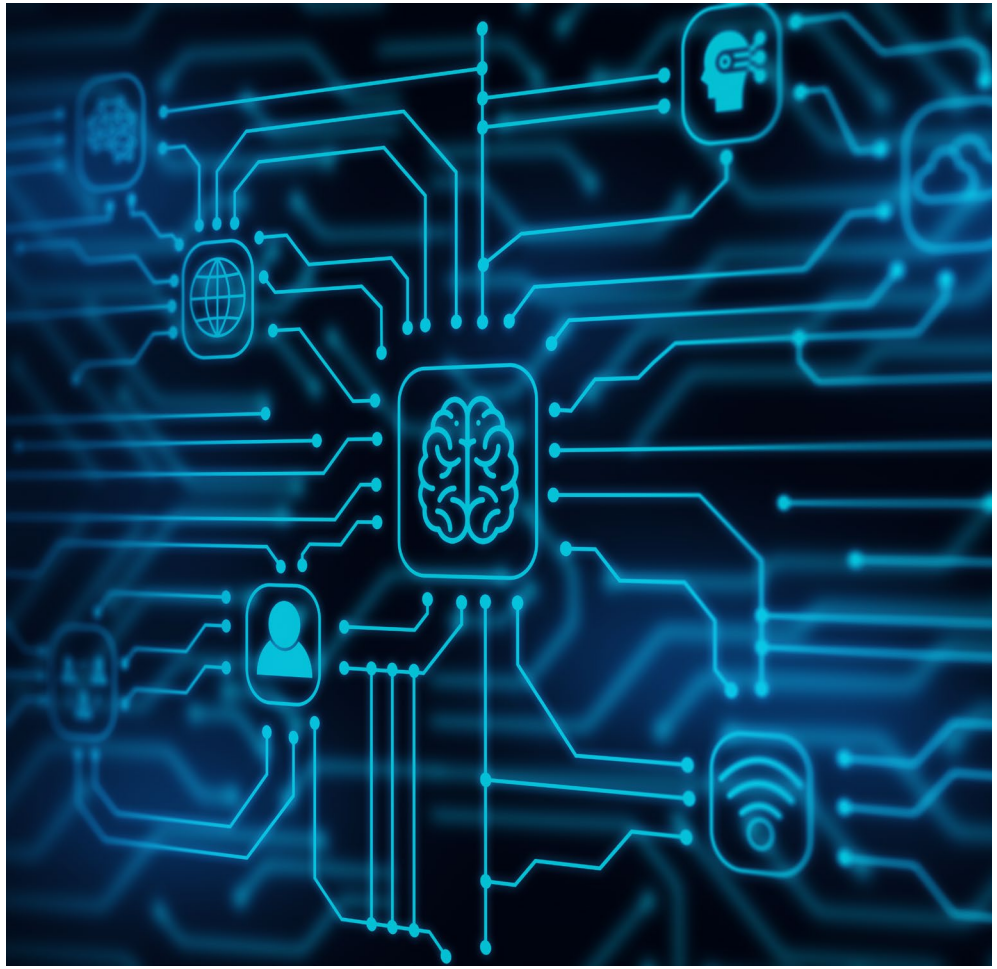
Product/Use Case Specific AI Issues

- Policies need to be customized for each company based on their use, **business** other company-specific factors
- Most “free” tools present unacceptable legal risk and typically not approved
- Develop approval/diligence criteria
- Many companies only permit use of approved products/version (some with conditions) and use cases – ban others
- Publish process for seeking approval
- Use cases – some use cases carry greater risks (legal or business) and may not be approved
- For lawyer use – factor in ethical issues

Bonus Topic – AI Agents

- AI agents present a host of **serious** legal and business risks (e.g., AI shopping agents) - need to understand and manage these risks
- Amazon sued Perplexity to prevent user created purchasing agents from transacting on Amazon
- N.D. Cal. issued PI (stayed pending appeal): cannot access platforms without owners' permission - found strong evidence that Perplexity had *user's permission* but accessed user's password-protected accounts, *without authorization from Amazon*
- **Companies need to assess their websites technology to deal with agents and update ToS**
- **Employee use of AI agents must be addressed in AI policy!**

Agentic AI Commerce: The Next Wave of Online Shopping and Retailer Risk



Questions & Answers

Jim Gatto

AI, Robotics and Quantum Team Leader

jgatto@sheppard.com

703-989-9288

Please connect on LinkedIn

Reach out for custom AI presentation for your company

See articles on Artificial Intelligence

Subscribe to blog for updates