



AI: Mitigating Legal Risks and Liabilities

Presented By: Lyle Gravatt

November 13, 2025



Overview

- Understanding AI
- Legal Implications
- Use Cases
- Best Practices
- AI-related Legal Needs

Understanding AI

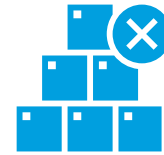


What is Artificial Intelligence (AI)?

Artificial Intelligence (AI):



Mimics human
intelligence



Finds patterns,
understands
natural language



Learns from data
input, adapts

Generative AI (GenAI): user prompts generate new, “original” content (e.g., text, images, music, videos).

Model: algorithms applied to vast amounts of data to learn patterns and insights, and make predictions and decisions (outputs) based on user inputs (prompts).

AI Components

INPUT INFORMATION → PROCESS INFORMATION → OUTPUT WORK

Input: iterative process – user prompts, outputs, and feedback may continuously improve the model.

Process:

- inputs may be compressed, revised or otherwise manipulated.
- statistical-based analysis instead of traditional logic.
- reinforcement learning – feedback encourages/discourages repeat behavior.

Output: content generation (GenAI), judgement, prediction, analysis, or any number of decisions or actions.

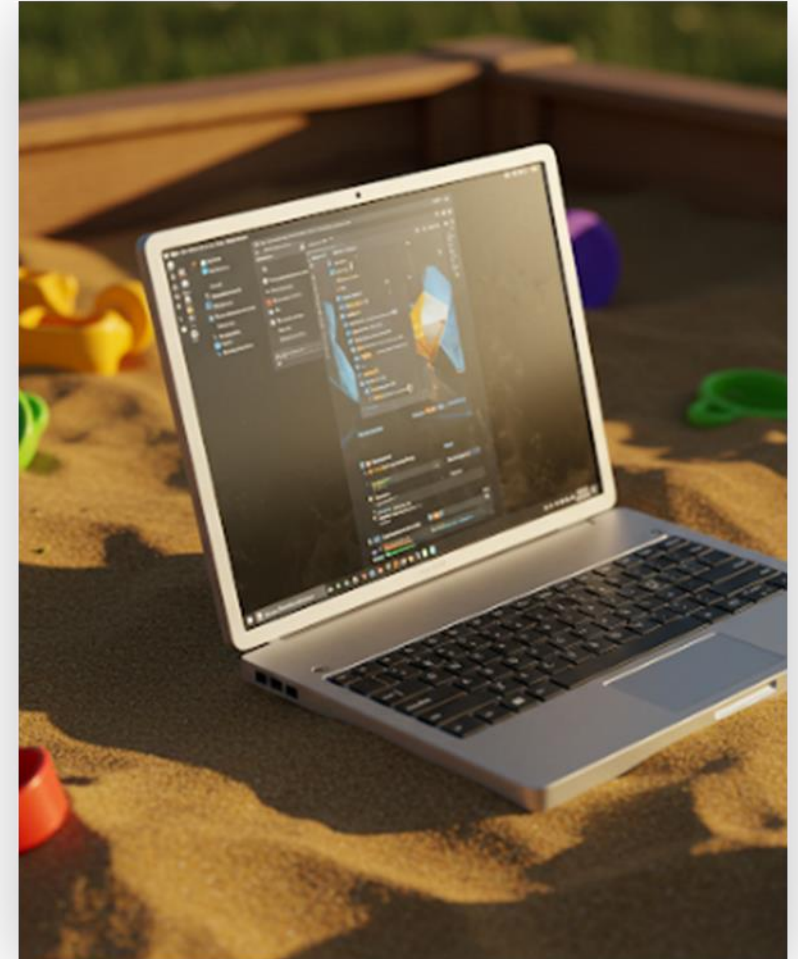
Public vs. Private AI

Public AI (aka open AI)

- Unrestricted Access - can be used by anyone (though some are paid services).
- Unrestricted Data Use - any inputs could become an output.

Private AI (aka sandbox AI)

- Restricted Access - limited to subscribing entity's users
- Restricted Data Use – inputs not accessible by third-parties, though they may be used to develop a private model for the subscriber.



Why All the Hype?

Speed – Efficiency – Ease-of-Use – Trendy

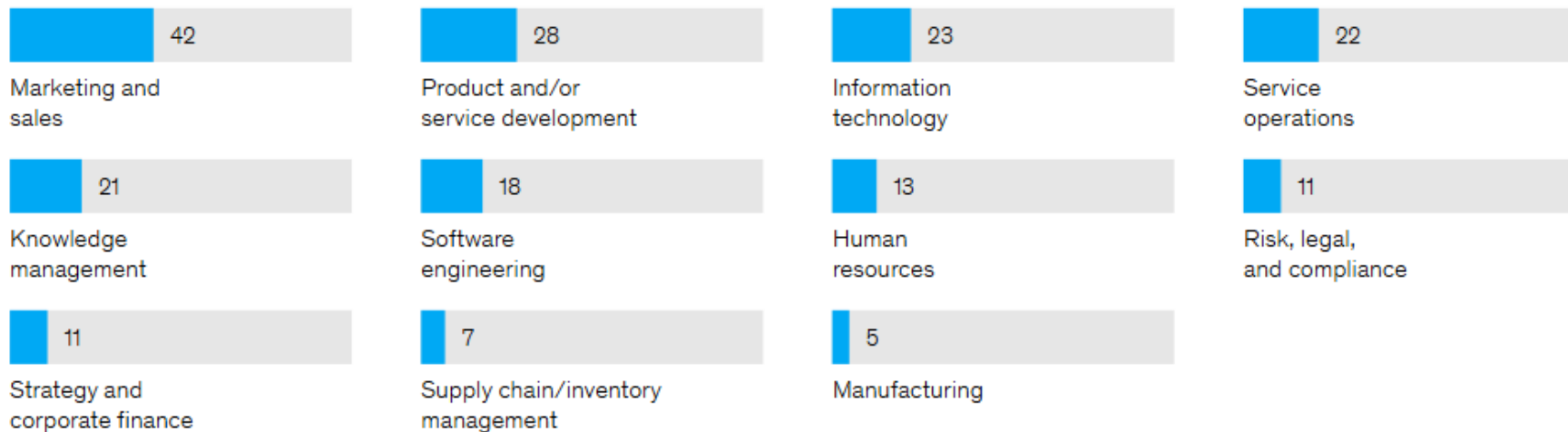
- **Content Generation** – creating text, video and audio based on user prompts for research, advertising and marketing.
- **Speech and Text** – conversion, language translation.
- **Efficiency** – streamline processes, enhance visibility and responsiveness.
- **Evaluation and Analysis** – sensing, recognizing and pouring through large amounts of data.

Rapid Adoption – Businesses

In a recent McKinsey survey, 71% of respondents said their organizations use generative AI in at least 1 business function, although only 1% of executives describe their AI use as “mature.”

Note – employees are early adopters, often using tech solutions before adoption by their employers.

Use of gen AI by business function, % of respondents



Rapid Adoption – In-House

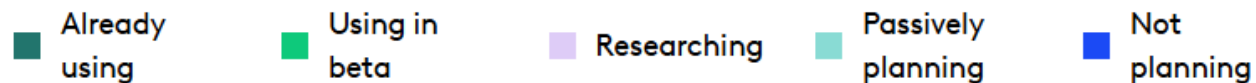
Are you currently using, or planning to use, generative AI in your legal work?

YOY Changes

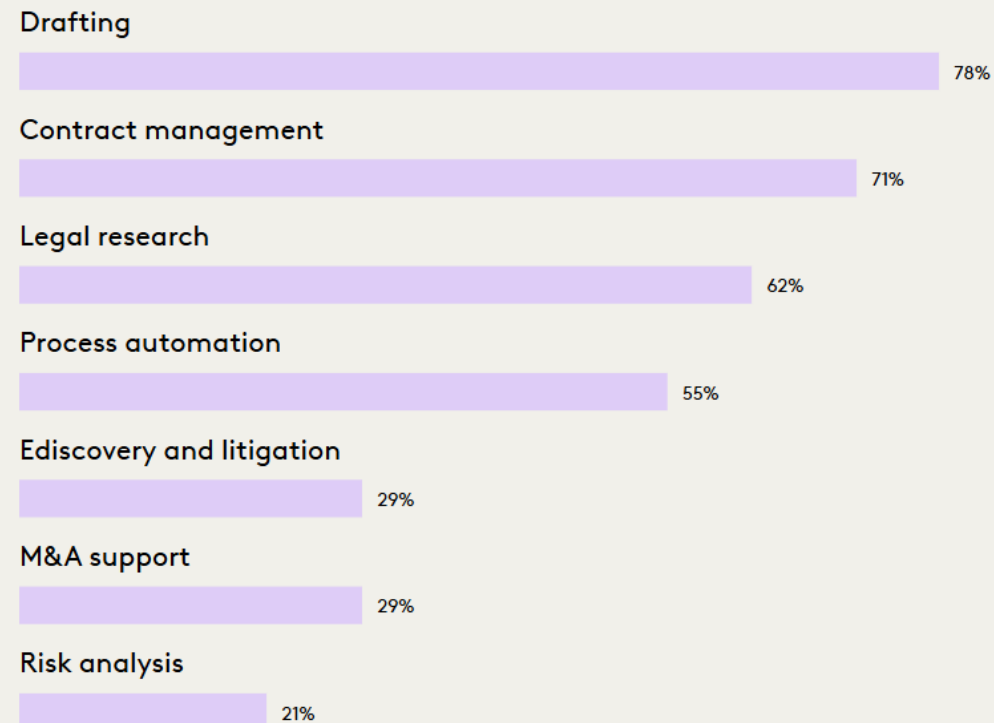
2024



2025



What type of legal work do you see the greatest opportunity to handle in-house with GenAI?



Legal Tools

Contract Management

Summize Corpora Sirion
Ironclad Uncover fynk
SPOTDRAFT Evisort lexion
Avokaado Juro ContractPodAi

Legal Research & Intelligence

deepjudge eve alexi DocLens.ai
AMICUS wexler.ai PAXTON
LEXLINK.AI responsiv descrYbe.ai
patterndata LAER.AI
Casetext CALLIDUS Beagle

Document Drafting & Negotiation

ThoughtRiver Robin AI
PINCITES ContractAI
Spellbook definely Syntheia
henchman Luminance
SPEEDLEGAL ontra recital
DocDraft trusli Clearbrief
Briefpoint FirstRead

Workflow Specific

Josef Scribe TRUE LAW
LegalFly Rhetoric bench iq
LEGALMATION EvenUp Harvey.
Composure

IP Management

IPRally patsnap trade space
BLACKHILLSAI Questel

IP Protection & Monetization

Patented ScaleIP
MARQVISION
IP COPILOT xlscout

Patent Drafting & Review

garden Patlytics
Edge PatentPal
LightbulbML Solve Intelligence

Patent Research

ambercite Amplified pqai
chekable NLPatent

Legal Implications



AI Inputs & IP

Trade Secrets and Confidential Data – any information provided to any AI service creates risk of dissemination (obtain consent to de-identify, aggregate, create derivative data, and use for purposes of training AI).

- Attorney-Client Privilege (consider access)

Copyright and Trademark Infringement

- Uploading third-party images or art as ‘inspiration’.
- Inputting sets of publications (also consider service terms).

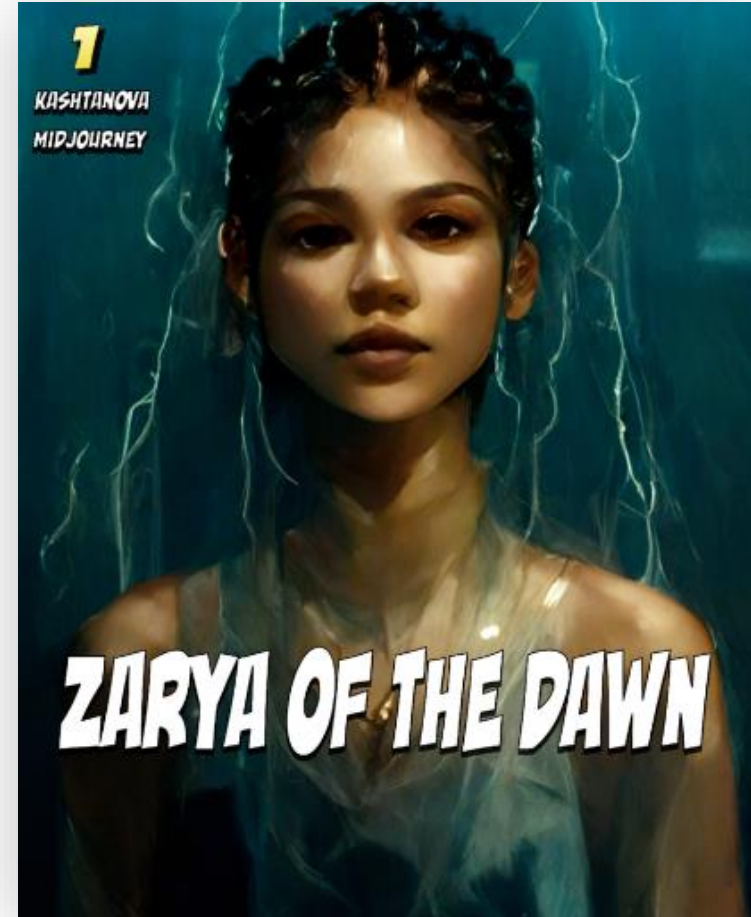
AI Outputs & IP

Ownership

- U.S. - AI-created portions of works are not copyright protected.
- Consider implementing processes that encourage human authorship.
- U.S. Copyright Office requires applicants to explicitly disclose AI-created portions.
- China/U.K. - allow for protection of AI-generated works.

Enforcement and Protection - without ownership, there are no rights to enforce.

Unfair Competition / Unjust Enrichment – user prompts that attempt to mimic others or intentionally extract protected information could create liabilities.



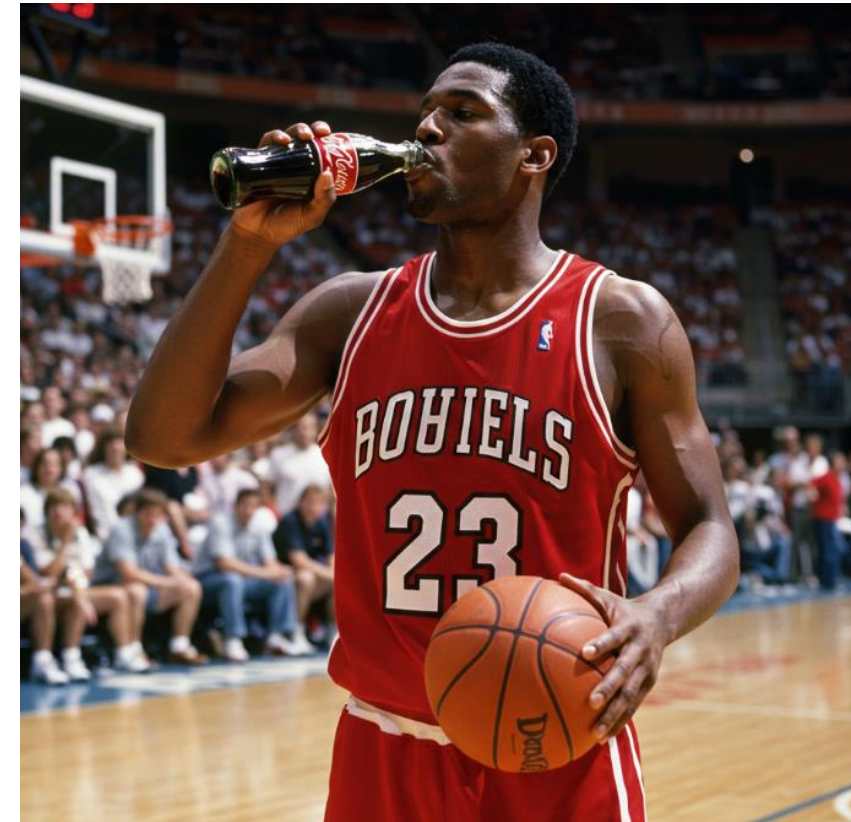
AI Outputs & IP

Infringement Concerns

- Are the outputs substantially similar to a third-party's copyright-protected work?
- Are third-party trademarks embedded in images?
- Are publicity rights being implicated?

Best Practices

- Keep a 'human in the loop' to review content before dissemination or action.
- Revise and edit.
- If there are repeated violations, consider additional training.
- Tracking prompt inputs as evidence of (un)intentionality.



Transactional Issues

Data Privacy – personal identifiable information (PII) is highly regulated, as is other sensitive data (health, biometric, etc.).

Contracts – consider third-party contract terms addressing confidentiality, AI use and work product ownership.

Terms of Use from

- AI service provider (and the AI model provider, if different).
- Any third-party platform from which data may be collected.

Regulatory Concerns

SEC, FTC and CFPB – “AI washing” concerns, involving misrepresenting the AI capabilities of a business, product or service.

EEOC – strong focus on potential discriminatory hiring practices.

FDA – transparency on algorithmic decision-making (e.g., medical devices)

State Legislation – some have regulated large, advance AI models, while others are focused on niche uses (e.g., political campaigns, minors, pornographic).

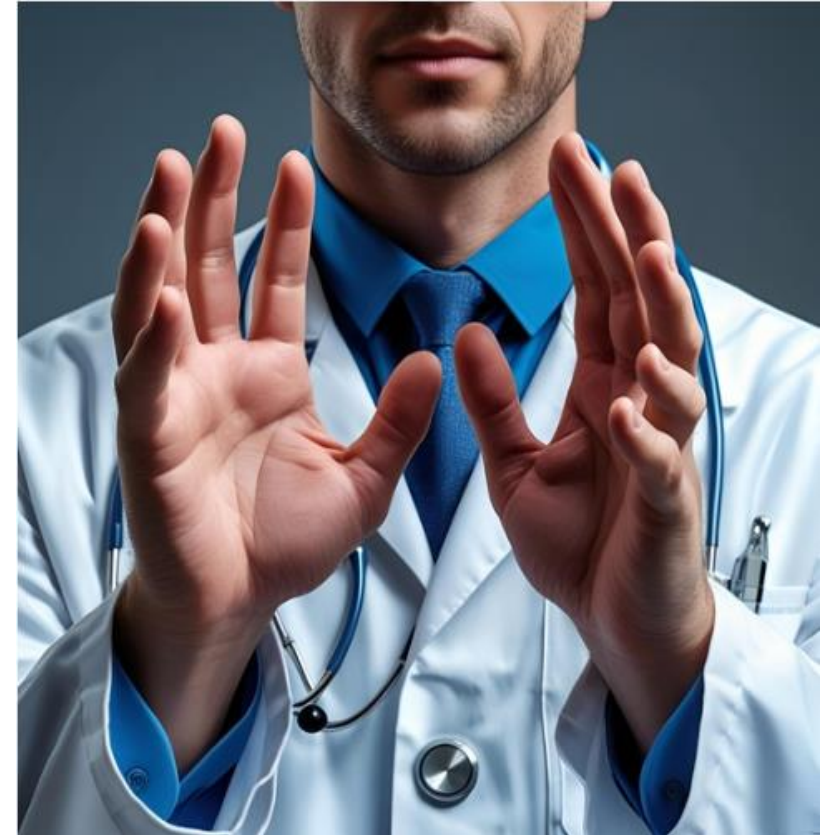
Other Liabilities

Bias – AI model is only as accurate as training data and inputs.

- Unconscious - same bias as in training data (data samples may not be representative of totality).
- Temporal - not reflective of changes or shifts in behaviors or trends over time.
- Edge-case - fails to account for rare or unusual examples.

Misinformation – AI outputs are statistical calculations, so some errors are expected; “data poisoning” of AI models.

Public Relations – public perception of AI is both positive (cutting edge) and negative (mistrust, ridicule).



Use Cases



General Use Cases

- Drafting Written Works
- Image Recognition and Creation
- Research and Ideation
- Document and Data Analysis
- Monitoring and Predictions
- AI Influencers

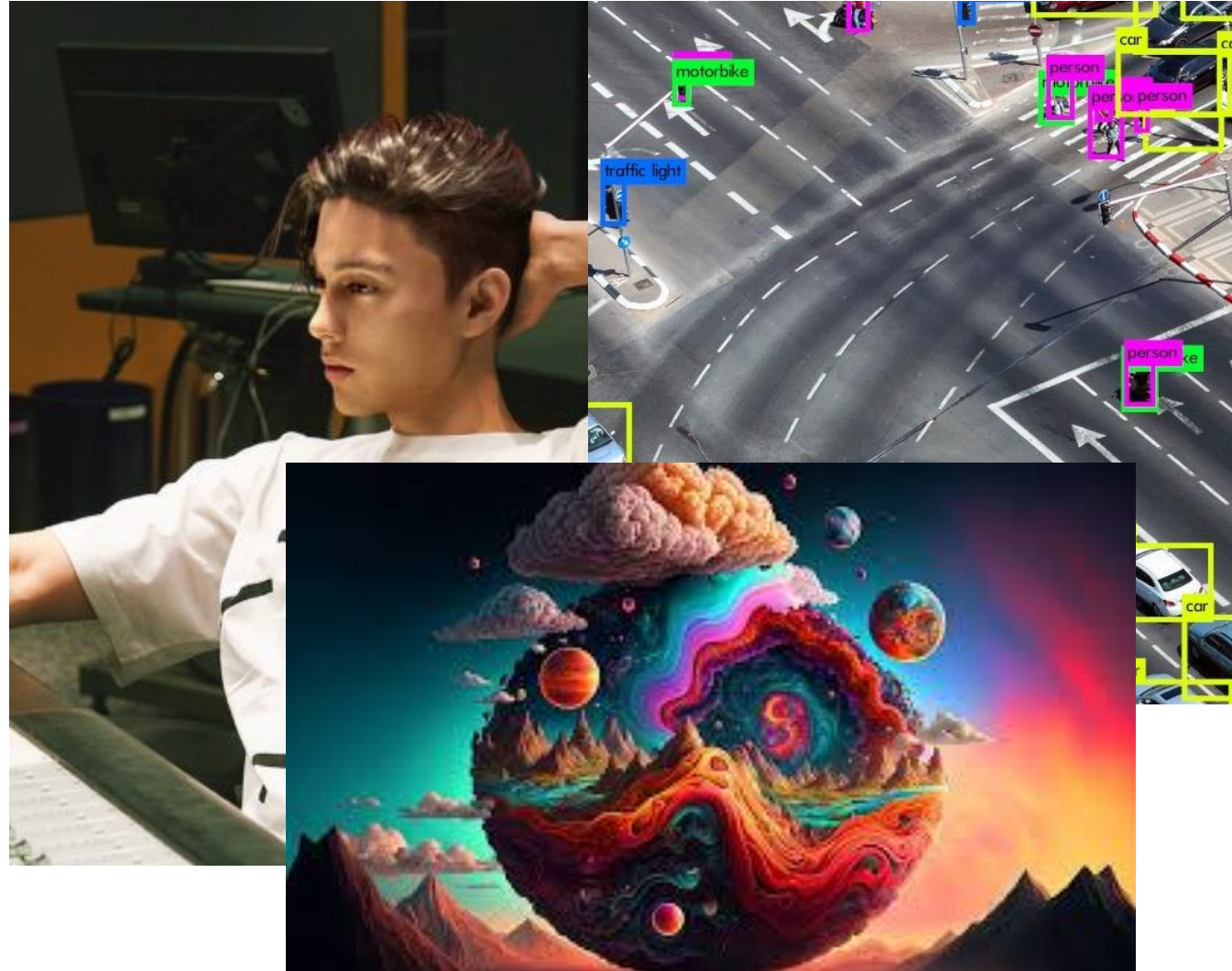
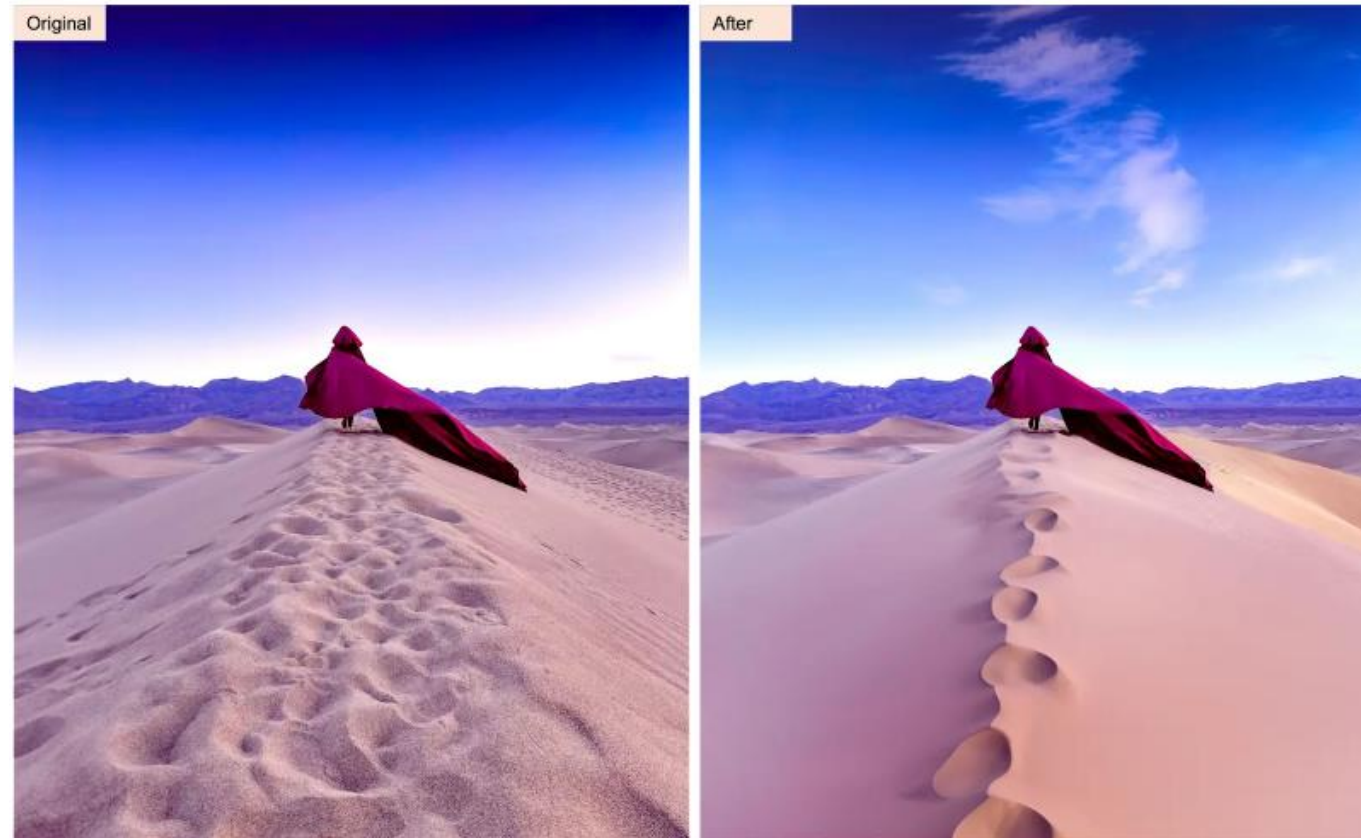


Image Editing

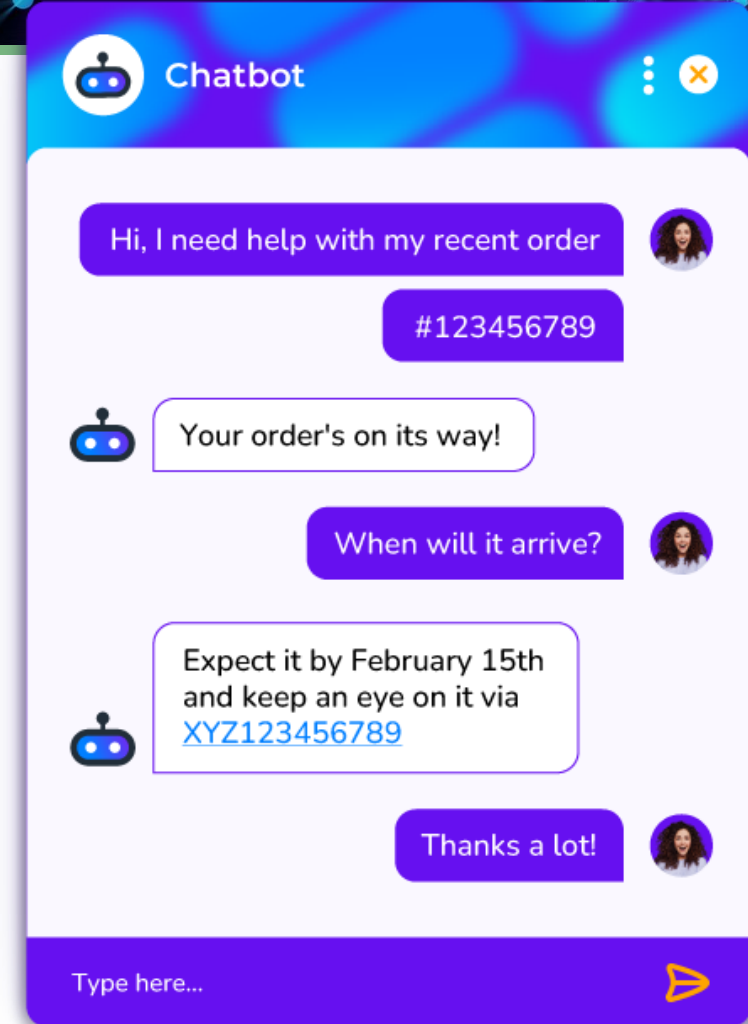


Source: <https://blog.adobe.com/en/publish/2023/05/23/future-of-photoshop-powered-by-adobe-firefly>

CA's AB 853 (effective Aug, 2026) – detects and watermarks AI content on large online platforms.

Chatbots

- Very popular online and via apps.
- Users unlikely to review terms of use and privacy policies.
- Misinformation and bias more prevalent.
- Cybersecurity risks – social engineering, phishing, malware.
- CA's SB 243 "companion" chatbot protocols and notices (does not include customer service chatbots).



Meeting Transcriptions

- Offers live transcription or translation, meeting summaries and takeaways.
- Output stored for later use, accessible by various parties.
- Consent, confidentiality and litigation concerns.
- Business concerns – chilling, hyperbole, overreliance.

Summary

The purpose of the meeting was to discuss strategies for improving team building within the organization. The meeting was attended by the entire team, including the team leader, managers, and other members. Discussions included the importance of communication, trust, collaboration, and appreciation.

Topics

- Importance of effective communication in building a strong team
- Strategies for building trust among team members
- Importance of collaboration and teamwork in achieving common goals

Action Items

- Develop a communication plan to improve team communication
- Schedule regular team building activities and exercises
- Provide training on effective teamwork and collaboration

Key Questions ⓘ

- What are some team building activities that we can do as a team?
- How can improve communication within the team?

Human Resources

High Risk

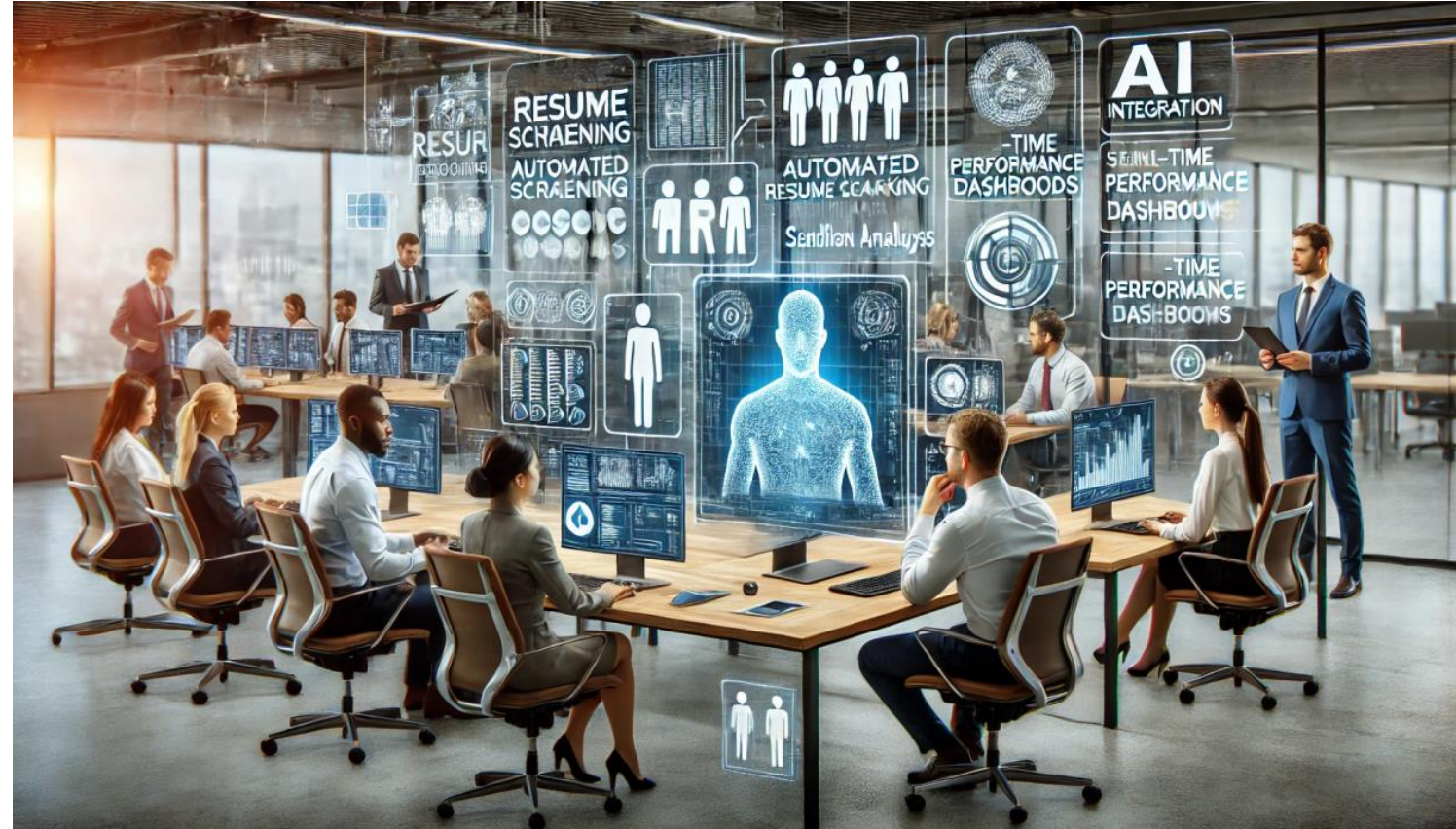
- Recruiting and Talent
- Employee Engagement and Retention

Medium Risk

- Performance Management
- Payroll & Benefits

Lower Risk

- Onboarding Automation
- Learning/Training
- Document Management



Best Practices



Preparation

Alignment amongst leadership, workers, and organizational principles and risk tolerance.

AI Governance - create a cross-functional (inter-departmental) AI leadership team to ensure ethical, accountable, and transparent AI use.

Proactively Engage and Educate workers, vendors, contractors and customers to build trust, address concerns, and reduce risk.

Technical Capability – ensure adequate expertise and infrastructure; consider data governance generally (access, cybersecurity, structure).

Contractor Concerns

Review historical relationships to ensure contracts address AI-specific concerns, namely confidentiality, IP ownership, reps/warranties, indemnifications/liabilities.

Confidentiality - consider language noting AI concerns as contractors may not be aware of confidentiality risks.

- Prohibit AI Use - Recipient may not process Confidential Information using AI.
- Permit AI Use - Recipient may process Confidential Information using AI under certain conditions.

Ownership - if AI use is permitted, contractor should explicitly and clearly identify any deliverables generated by AI.

Adoption

AI Acceptable Use Policy – address pre-approved tools and uses, access terms, required training, reporting structure and best practices.

Vendor Policies – review vendor contracts, terms of use and privacy policies (even historical vendors that may be newly adopting AI features or tools); audit internal use of AI.

Business Impact – review and understand specific AI solution requirements and how it may be most impactful to specific:

- organizational problems or processes;
- liabilities, legal concerns, tech/data/other agreements; and
- data governance (access, cybersecurity, structure).

Vendor Concerns

Assess - consider impact on internal processes, infrastructure and data access rights.

Terms of Use and Privacy Policies - in many cases the language is informative and not up for negotiation; consider reps, warranties, indemnifications, liabilities, and confidentiality.

Burden On User - typically responsible for liabilities associated with inputs and outputs.

Third-Party Providers - many AI features are 'powered by' third-party AI technology; may implicate additional policies.

Implementation

Iterative Approach (Crawl, Walk, Run) the regulatory environment, worker and customer knowledge, and AI functionality will evolve at a rapid pace.

Learn – seek and communicate knowledge about AI, specific AI tools, use cases, prompt engineering and best practices; engage super-users.

Adapt rapidly to regulatory environment, worker and customer feedback, and new features and updates to the AI tools.

External Concerns – consider pro-active steps to mitigate impacts on customer service, vendor relationships and branding/public relations.

Takeaways

- **Work Email** - always login using your work email.
- **Inputs** – consider data privacy and confidentiality issues (obtain consent if recording).
 - Prompts can lead to efficiencies and create risk.
- **Output** – always have a “human in the loop” to review before taking action or disseminating.
 - Consider how AI may inspire creativity or quickly identify potentially relevant information.
 - Always be wary about accuracy, misinformation or 3rd party rights.
 - Generally, not protectable; introduce authorship.



AI-related Legal Needs



AI-related Legal Needs

- **Intake and Awareness** – an initial conference with client to intake their goals and concerns, and raise general awareness of AI legal concerns.
- **Education and Training** – a presentation to a larger group to provide more thorough knowledge of AI legal concerns and offer some best practice tips.
- **Periodic Updates** – additional conferences may be desired, depending on level and complexity of AI adoption and use.
- **AI Acceptable Use Policy** – recommended for all clients; addresses pre-approved AI tools and uses, access terms, required training, reporting structure and best practices.
 - Typically separate from handbook and any other technologies policies.

AI-related Legal Needs

- **Independent Contractors** – review and update agreements with third-parties to address AI-specific legal concerns, particularly confidentiality and IP ownership.
- **AI Vendor Agreements** – review AI tool terms of use and privacy policies; assist client in negotiating favorable licensing terms.
- **Data Governance** – the data privacy team may assist with a number of AI-related data concerns, including compliance, sensitive or protected data, cybersecurity, access management, and third-party interactions.
- **AI Tool Development** – significant number of additional liabilities that arise when AI tools are developed and operated by a client, which may involve software and licensing agreements, state and federal AI regulations, and general bias and IP concerns.

Questions?

