PHOENIX
BUSINESS JOURNAL

HOOP DREAMS

With four No. 1 seeds in town, Phoenix could see an unprecedented economic boost from the Women's Final Four

BRANDON BROWN,
PAGES 14-16

PHOENIX BUSINESS JOURNAL • April 3-9, 2026, Vol. 46, No. 35

PHOTO ILLUSTRATION BY CERISSA LINDAY | PBJ; GETTY IMAGES

THE LIST

This week we rank nonprofit executive pay, manufacturers and more

PAGES 22, 24, 25

DEVELOPMENT

Gilbert project seeks restaurateur

A prominent retailer is looking to build out a unique space in the Heritage District

BRANDON BROWN, 3

GOVERNMENT

Data center rules could be costly

Some Phoenix landowners are seeking compensation with new rules in place

HAILEY MENSIK, 6

Confidentiality Issues in the Age of AI Tools

The Legal PULSE

JOSHUA BECKER
Shareholder
Gallagher & Kennedy

Joshua Becker is a shareholder at Gallagher & Kennedy with more than 20 years of experience in franchising and intellectual property law. He helps companies of all sizes across a myriad of industries protect and commercialize their valuable IP assets through domestic and international license agreements, trademark registration and maintenance, copyrights, and internet protections and procedures. Whether a client is creating, growing, buying, or selling their business, Josh is skilled in negotiating and closing licensing agreements, franchising deals, M&A, entity formation, joint ventures, and other commercial agreements of all kinds.

Gallagher&Kennedy
gknet.com

Artificial intelligence (AI) is embedded in the daily work of companies of all sizes, shapes, and locations. Your employees, vendors, partners, prospective acquisition partners, suppliers, and customers are all using, knowingly or unknowingly, AI as part of their job functions and core business models. Those habits collide with two issues not included in many traditional confidentiality agreements: (1) inadvertent breach of confidentiality obligations through use of public AI tools, and (2) the ownership of AI outputs. Because courts have not provided clear guidance on the implication of AI usage, businesses have little common or statutory law to rely on. Drafting thoughtful agreements is key to protecting your valuable IP assets and avoiding claims that you failed to protect the IP assets of others.

This article briefly summarizes the issues, the current legal landscape, and pragmatic steps to protect your valuable IP and insulate your company from claims that you breached confidentiality obligations.

REDUCING THE RISK OF UNINTENTIONAL DISCLOSURES

The default setting for public facing, free versions of OpenAI, Gemini, ClaudeAI, and similar platforms allows them to use your inputs to train their models. Users must take overt steps to instruct these tools to not use inputs for training and development. The possibility that confidential information may be used to generate additional ideas, concepts, plans, strategies, or code; and that unrelated and unaffiliated third parties may view the information—even under confidentiality agreements—may constitute an unauthorized disclosure.

Enterprise platforms (e.g., Microsoft 365 Copilot with Enterprise Data Protection, Google for Gemini Cloud, Amazon Bedrock, Anthropic Enterprise, etc.) generally operate under data processor terms, do not use prompts or content to train foundation models, and therefore materially reduce risk of unintentional breaches. Most enterprise AI offers contractual guarantees that: (1) customer data is not used for training; and (2) data is isolated within the tenant environment.

Confidential information should never be inputted into non-enterprise or public AI systems. For example, an employee pastes a customer price list into ChatGPT to evaluate whether the pricing is consistent with market trends. Even if the prompt is later deleted, the disclosure may still violate the confidentiality agreement because the platform retains safety monitoring logs.

Without proper education or prompts, your employees may not understand the difference, and can put your company at risk of violating its confidentiality obligations.

OWNERSHIP OF AI OUTPUT PRODUCED BY AI TOOLS

While there is an understandable focus on protecting the confidentiality of delivered information, confidentiality agreements must now also address conflicting ownership claims by the recipients of confidential information when that recipient uses AI to create summaries, analyses, reports, recommendations, or code.

Traditional "work product" language in vendor agreements may push AI outputs into the recipient's ownership. This issue becomes more complicated because AI generated content does not reliably qualify under U.S. copyright law. Under current U.S. laws, copyrights require a human author to qualify for copyright protection. Outputs produced solely by AI may therefore not be protected as derivative works under copyright law and may not be captured by "derivative works" language in a confidentiality agreement. Because derivative work protections cannot be reliably assumed, lawyers should rely on contract language—not copyright law—to establish ownership. If ownership provisions are unclear, the receiving party may later assert that AI generated outputs constitute their own work product, especially where their service agreements contain broad IP ownership clauses or ambiguous "work made for hire" language.

Vendors, consultants, developers, and even prospective acquirers may input your confidential information into an AI platform to produce summaries, analyses, drafts, recommendations, or code. The AI output from such an exercise may be valuable, novel, or an extension of your business plans and trade secrets. If your confidentiality agreement is silent, the recipient might assert that these AI assisted outputs reflect their own independent work product or are owned under their general service provider terms. These outputs may not be covered by traditional "derivative works" clauses as AI outputs may not qualify as derivative works under U.S. copyright law.

IMPLEMENTATION STEPS

1. To avoid inadvertent breaches and protect your company's IP, confidentiality agreements should:
2. Identify clear rules for employees and contractors (no uploads of confidential information to public AI).
3. Authorize only enterprise or private deployments of AI tools with contractual no-training guarantees.
4. Prohibit the use of public chatbots with confidential information provided pursuant to a confidentiality agreement and further require recipients to obtain separate written authorization before inputting confidential information into a private or enterprise AI tool. This prevents both unauthorized disclosures and future ownership disputes.
5. Specify that the disclosing party owns all outputs-whether created by humans or AI-based on, derived from, or generated using the disclosing party's confidential information.
6. Include language that all return and destruction obligations apply to AI-generated analyses, drafts, summaries, recommendations, or code.

The evolution of AI requires confidentiality agreements to include explicit contractual language governing ownership, permitted uses, and destruction of AI generated outputs. Clear drafting prevents disputes over ownership, scope of use, and the treatment of materials generated using a company's confidential information.