Phelps Dunbar LLP
Canal Place
365 Canal Street, Suite 2000
New Orleans, LA 70130
504 566 1311

Protecting Company Trade Secrets in the Age of AI

As employees increasingly rely on generative artificial intelligence (Gen AI) tools, companies face a growing risk of confidential information being exposed, stored or reused by these systems. This could undermine trade secret protection. Recent court cases and high-profile disputes underscore the need for "reasonable measures" to maintain secrecy to evolve alongside technological advancements.

In-house counsel should consider these risks and implement AI-specific confidentiality policies, train employees, update agreements, and consider other measures to safeguard proprietary data and preserve legal protections under federal and state law.

The Rising Trade Secret Challenge in the AI Era

Gen AI tools, such as ChatGPT, Gemini and Copilot, have transformed how employees draft documents, analyze data and generate ideas. However, their ease of use introduces new risks. Employees may inadvertently feed proprietary or client information into public AI systems that retain or learn from those inputs. Once information is outside the company's control, its "secret" status may be compromised, along with protections under trade secret law. Along those same lines, if a "trade secret" can be easily extracted with a common-sense prompt using a public Gen AI tool, it may not even be considered a "trade secret" as defined by federal or state law. In this evolving landscape, legal departments must balance harnessing AI's benefits with enforcing controls to keep proprietary knowledge confidential and understanding what data may not be protected.

When AI Turns Data Into Disclosure

Public AI tools often retain user inputs for model improvement. When employees input confidential materials, such as source code, pricing data, training data, or client names or contact information, into these systems, employees may unintentionally share trade secrets with platform operators. Even when an employee uses closed AI models, these programs can "learn" and later reproduce portions of data. Consequently, an AI tool might unknowingly echo confidential logic or information in responses to others, even within the company, who may not understand or appreciate the need for confidentiality. Even closed AI models can fall victim to "prompt injection" attacks, a form of cyberattack particularly damaging to AI systems. In these attacks, hackers or other malicious actors craft prompts designed to circumvent the safeguards of a Gen AI system, potentially leading it to reveal confidential and proprietary information.

Legal Backdrop: The 'Reasonable Measures' Standard

The term "trade secret(s)", as defined under Federal Law, has three parts: (1) information; (2) reasonable measures taken to protect the information; and (3) which derives independent economic value from not being publicly known. Defend Trade Secrets Act, 18 U.S.C. §1839(3)(A), (B)(1996). As a result, under the Defend Trade Secrets Act and state law (as most states have adopted some version of the Uniform Trade Secrets Acts), companies must demonstrate they made reasonable efforts to keep information secret and not publicly known. AI complicates this analysis. Most companies' confidentiality agreements and employee handbooks predate Gen AI. Without explicit policies restricting what can be shared with AI tools,

it becomes challenging to address misconduct in using AI tools and prove that the company took the "reasonable measures" required by trade secret law. If employees can freely use public tools without guardrails, courts may find that the company failed to protect its secrets.

Cases addressing whether company information published on the Internet constitutes trade secrets may be analogous to the use of public AI tools. *See, e.g., Keane v. Fox Television Stations, Inc.*, 297 F. Supp. 2d 921, 941 (S.D. Tex. 2004), *aff'd*, 129 F. App'x 874 (5th Cir. 2005) ("[Plaintiff's] additional factual assertion that he advertised his 'American Idol' concept on the Internet entirely eviscerates his ability to characterize that concept as a trade secret or as an idea that was conveyed in confidence to a select group."); *CDX Holdings, Inc. v. Heddon*, No. 3:12-CV-126-N, 2012 WL 11019355, at *6 (N.D. Tex. Mar. 2, 2012) ("[T]he list of clients does not qualify as confidential information because there is evidence showing that [Plaintiff's] customer identities are public information accessible through its website. Information that might otherwise be considered a trade secret loses that status if it is well known or readily available to the public.") (finding plaintiff unlikely to succeed on merits of trade secret appropriation claim and denying motion for preliminary injunction); *Vibraderm, Inc. v. Multiderm, L.L.C.*, No. 3:07-CV-1331-M, 2008 WL 11425397, at *2 (N.D. Tex. Mar. 26, 2008) ("[C]ontact information of [Plaintiff's] clients was published on Plaintiff's website and thus is not a trade secret.").

Practical Safeguards for In-House Counsel

1. *Create a Clear AI Use Policy*: Define approved AI tools and explicitly forbid employees from inputting sensitive data into unapproved or public systems and using unapproved devices. Require employee disclosure of AI use. Foster collaboration between legal, IT and HR departments to ensure a cohesive approach to trade secret protection and policy enforcement.
2. *Educate and Train*: Implement regular training sessions to educate employees about the importance of trade secrets and the specific risks associated with AI technologies. Ensure that employees (and applicable third parties) understand the potential legal consequences of mishandling sensitive information.
3. *Use Secure Platforms*: Adopt enterprise-grade or internal AI systems that are password-protected, guarantee data isolation, and prohibit model training on your inputs. Have a plan of action in place to respond swiftly in the event of a breach.
4. *Update Contracts and NDAs*: Revise confidentiality provisions with employees, contractors and vendors to explicitly cover AI-related risks, including the use of AI training data, prompts and model outputs. Prohibit users of the company's AI model from reverse engineering the model to learn its data or reproduce its processes. Consider other options to protect proprietary information in the event a court determines that the information is no longer a trade secret, such as implementation of nonsolicitation, noninterference, and noncompetition agreements.
5. *Monitor and Audit*: Stay informed on changes in the AI landscape and conduct regular audits of AI systems to identify and rectify vulnerabilities. Ensure that AI configurations adhere to the company's data protection policies and industry best practices.
6. *Document Your "Reasonable Measures"*: Maintain records of employee training, policy dissemination, access controls and vendor certifications. Documentation can be pivotal if litigation arises.

AI offers tremendous promise; however, without careful controls, it can also become a conduit for unintentional trade secret loss. As AI revolutionizes industries, protecting trade secrets must remain a top priority for businesses. By understanding the risks, implementing proactive measures, and staying current as AI technology evolves, legal departments can safeguard their company's competitive edge in an increasingly digital world.

About the Authors

A board-certified labor and employment lawyer by the Texas Board of Legal Specialization, Claudine Jackson has spent more than 25 years advising company management on workplace and employment law issues. Informed by experience as a former in-house employment counsel for an international corporation, Claudine helps executives make decisions with an eye on the business implications. She's often called on to defend clients in federal and state courts, arbitration and before the EEOC, Department of Labor, Texas Workforce Commission and Texas Education Agency.

Claire Monsour is an associate attorney in Phelps' Fort Worth office and part of the firm's regional labor and employment group. While in law school, Claire trained as a student mediator and resolved disputes involving litigants in city court. She served as a research assistant for an employment law professor and as managing editor of the *LSU Law Journal for Social Justice and Policy*.