JS|HELD

PERSPECTIVES

TRADE SECRET PROTECTION IN THE AGE OF LARGE LANGUAGE MODELS:

Risks, Reasonable Measures, and Legal Remedies

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

Introduction

Large Language Models (LLMs) are a type of Artificial Intelligence (AI) system that can process and generate human-like text based on the patterns and relationships learned from vast amounts of text data[1]. LLMs use a machine learning technique called deep learning to process text data from books, articles, web pages and other sources[2]. Context Windows are the space or memory available for users of LLMs to prompt a response. In addition to these data sources, LLMs may analyze and process the text users enter in context windows – which are typically large enough for a few thousand words – for model training and improvement[3]. This presents unprecedented risks to trade secret owners as proprietary information may be inadvertently or maliciously publicly disclosed through use of LLMs and context windows. As LLM solutions continue to evolve, organizations should continue to evaluate policies and procedures that protect against these related risks.

This article examines how LLMs process text and potentially disclose trade secret information; the potential adverse impacts of the disclosure of trade secrets by LLMs; the reasonable measures trade secret owners may implement to protect against this risk, and the remedies available to trade secret owners when proprietary information is inadvertently or maliciously disclosed via LLMs. We also discuss potential discovery strategies in litigation, address how the disclosure of trade secrets via LLMs is like other types of disclosures[4] and evaluate insurance coverage options.

Open-AI released the first LLM, known as GPT-3, in 2020[5]. Today, ChatGPT-4.5 and other LLMs such as DeepSeek, Qwen2.5-Max, Grok 3, LlaMA 3.3, Claude, and Gemini 2.5 are commonly used by individuals, businesses, students, educators, and other organizations[6]. These powerful tools offer unprecedented capabilities for information processing and content creation. However, they also introduce novel risks to intellectual property owners, particularly concerning the protection of trade secrets.

For many organizations, trade secrets represent a critical form of intellectual property, often comprising their most valuable and sensitive information – manufacturing processes, customer lists, algorithms, product formulas, customer-specific pricing, and other business strategies. Unlike patents or copyrights, trade secrets derive their value precisely from remaining confidential. Once publicly disclosed, they lose protection and value permanently.

How LLMs Process Text Data

Understanding how LLMs process text data is important to properly evaluate the risks they pose to the disclosure of trade secrets. LLMs use a machine learning technique called deep learning to process text from books, articles, web pages, and other sources[7]. Context windows are the space or memory available for users of LLMs to prompt a response. When an LLM user inputs information into a context window during a chat session, several processes within the LLM may create potential disclosure of proprietary information, including:

Input Processing: When text is entered into an LLM context window during a chat session, that text becomes part of the immediate conversation context. The LLM uses this context to generate output, referred to as “completions.”

Model Training: While the providers of most LLMs indicate that they do not utilize the text entered in context windows to train their LLMs without consent, policies vary significantly between providers. Some providers may utilize user text for model improvement, fine-tuning, or to enhance the quality of completions unless users explicitly opt out.

Data Storage: The text users input into context windows during chat sessions are often stored on providers' servers for a certain period. Even with the most robust security measures, this presents additional security risk to trade secret owners.

Pattern Recognition: LLMs are designed to recognize patterns within seemingly disparate textual data. A trade secret disclosed piecemeal across multiple chat sessions could potentially be reconstructed by an LLM as part of its completed response to related queries of third party users, even without explicit retention of the original texts containing the proprietary information.

The key vulnerability lies in the fact that once proprietary information is input into a public LLM, the trade secret owner loses effective control over that information. The LLM provider becomes an unwitting custodian of the data, with varying levels of safeguards against its public disclosure or use.

Potential Adverse Impacts of Trade Secret Disclosure via LLMs

The potential adverse impacts of the public disclosure of trade secrets through LLMs may be significant, and include:

Permanent Loss of Protection: Trade secret protection requires that the information remains confidential to the owner and not be within the public domain. Courts have consistently held that once a trade secret is within the public domain – regardless of how that disclosure occurred – the information permanently loses its status as a trade secret. This is different than disclosures to third parties which might be contained or redressed through an injunction or legal remedy.

Exponential Public Disclosure: Unlike traditional disclosures which may be limited to a specific business partner, vendor, customer, competitor, or publication, LLMs can potentially disclose proprietary information entered in context windows during "private" chat sessions with thousands or even millions of users worldwide, creating a non-containable exponential level of public disclosure. What is worse is that third party recipients of proprietary information via LLMs have no confidentiality obligations to the original owner. And it may be impossible to identify those who have accessed the information, making enforcement against subsequent users more difficult.

Loss of Competitive Advantage: By definition, trade secrets are protected as such because of the competitive advantage owners derive from their secrecy[8]. Once competitors gain access to the proprietary information through an LLM's completed response, this advantage is irreparably lost.

Adverse Financial Impact: The adverse financial impact of the loss of trade secrets may be significant. A 2023 analysis by Ocean Tomo of companies that comprise the S&P500 indicates that intangible assets commanded 90% of the combined market values as of 2020[9]. Thus, the public disclosure of key trade secrets may permanently impact a company's market value, especially companies driven by innovation.

Reputational Damage: Beyond the direct adverse financial impact, companies may sustain reputational harm and a loss of goodwill among customers, investors, other stakeholders, and the public at-large if valuable trade secrets are publicly disclosed.

The most grievous impact of disclosure via LLMs may be that a trade secret owner may remain unaware of the disclosure until the damage is done – when competitors implement similar processes, or when the once secret information becomes common knowledge within an industry.

Reasonable Measures to Protect Trade Secrets from LLM Risks

Organizations should consider implementing reasonable measures to protect against the risk of trade secret disclosure via LLMs by both corporate users and third parties.

A. Reasonable Measures for Corporate User Disclosures

Develop Clear LLM Usage Policies: Trade secret owners should establish clear corporate policies that identify the types of information that may and may not be input into the context windows of LLMs during chat sessions. These policies should explicitly prohibit the input of trade secrets and other proprietary business information[10].

Utilize Private or On-Premises LLM Solutions: Consider deploying private LLM solutions on-premises that operate entirely within the organization's secure environment, eliminating the risk of trade secret disclosure to external systems and third parties[11].

Implement Technical Controls: Deploy IT solutions capable of scanning and blocking the transmission of identified proprietary information through the context windows of LLMs, similar to data-loss-prevention (DLP) solutions.

Negotiate Carefully with LLM Providers: Negotiate agreement terms with providers of LLMs that specifically address data usage, retention, and confidentiality. Ensure the agreements include provisions that prohibit the use of proprietary information for model training and that require prompt deletion of text entered in context windows after the end of a chat session.

Compartmentalize Proprietary Information: Limit complete knowledge of trade secrets and other proprietary information to essential personnel only, reducing the likelihood that any individual employee could inadvertently or intentionally enter an entire trade secret into the context window of an LLM.

Periodic Training and Awareness: Educate employees about the risks associated with disclosing proprietary information during LLM chat sessions and provide clear examples of what constitutes appropriate versus inappropriate use of LLMs.

Monitor LLM Usage: Implement monitoring solutions to track employees' interaction with LLMs and regularly audit interactions for potential inappropriate use, including the disclosure of proprietary information.

B. Reasonable Measures for Third-Party Disclosures

Update Confidentiality Agreements: Update vendor / partner NDAs and employee confidentiality agreements to explicitly prohibit the input of proprietary information and trade secrets into the context window of LLMs or other AI solutions.

Utilize LLM and AI-Specific Agreements: When sharing trade secrets with vendors, business partners, or employees, execute agreements with provisions that prohibit the use of LLM and AI solutions to process, analyze, or store proprietary information.

Implement Usage Logging: Require partners and vendors to maintain logs of how and where your trade secret information is stored, processed, and accessed, including, for example, explicit prohibition of inputs in LLM context windows.

Regular Compliance Certification: Require periodic certification from partners and vendors confirming that they have not entered your trade secrets into an LLM solution or AI system context window.

Watermarking and Tracking: Where feasible, implement digital watermarking or other tracking mechanisms that help identify the source if confidential information is leaked.

These measures may help satisfy the "reasonable efforts to maintain secrecy" requirement of trade secret laws and create a stronger position for legal action if misappropriation occurs.

Discovery Strategies in Trade Secret Litigation Involving LLMs

As the legal landscape adapts to the challenges posed by AI and LLMs, attorneys handling related trade secret misappropriation disputes should consider novel discovery approaches:

Expanding Discovery Requests: Prepare and serve interrogatory and document requests that specifically address the defendant's use of LLMs or AI systems in relation to the asserted trade secrets. Sample language might include:

"Identify all instances where you input, uploaded, or otherwise provided the plaintiff's trade secret information or any portion thereof to a context window or other prompt of an LLM or AI system."

"Produce all transcripts, logs, other business records, and / or communications with any LLM or AI system regarding [specific trade secret subject matter]."

LLM Usage Logs: Request defendant's logs of LLM usage, including timestamps, prompts, and responses (i.e., completions) that might contain or reference the asserted trade secrets.

Forensic Analysis: Conduct forensic examination of defendants' servers, computers, and other devices to identify relevant interactions with LLM solutions during the relevant time periods.

Third-Party Subpoenas: Consider issuing subpoenas to LLM providers for records of the defendant's usage, subject to appropriate confidentiality protections.

Deposition Questions: Develop specific deposition questions addressing whether and how defendants utilized LLMs when working with the asserted trade secrets.

Expert Analysis: Engage experts who can analyze whether the defendant's outputs (products, processes, etc.) show evidence of being informed by LLM-processed versions of the plaintiff's asserted trade secrets.

This comprehensive discovery approach may help to establish whether trade secrets were entered into LLMs as part of a defendant's use, attempted design-around, or improvement of the asserted trade secret information.

Previous Cases Involving Disclosure of Trade Secrets

While disputes alleging trade secret misappropriation via use of LLMs are still emerging, previous disputes involving public disclosure through other means offer guidance:

Tekmira Pharmaceuticals Corp. v. Alnylam Pharmaceuticals, Inc.

The 2011 case of Tekmira Pharmaceuticals Corp. v. Alnylam Pharmaceuticals, Inc.[12] presents a scenario involving the public disclosure of trade secrets. In that case, Tekmira alleged that Alnylam improperly disclosed its trade secrets related to lipid nanoparticle technology for drug delivery in certain US patent applications. Alnylam originally obtained access to Tekmira's trade secrets through a collaboration agreement with Tekmira.

Ocean Tomo was retained to quantify Tekmira's recovery, which included the lost value of the Tekmira trade secrets allegedly disclosed by Alnylam. The case ultimately settled for USD 65 million[13] and established an important principle: a trade secret defendant may be liable for the public disclosure of a plaintiff's trade secrets even if the defendant originally gained access to and subsequently disclosed those trade secrets via seemingly legitimate means, such as through collaboration agreements and US patent applications.

This principle may apply to scenarios involving the use of LLMs. For example, a party that inputs another's trade secrets into a context window or similar LLM prompt which results in the public disclosure through subsequent LLM responses to third parties, could face similar liability and damage claims based on lost value, as in the Tekmira case.

Group One, LTD v. Hallmark Cards, Inc.

In Group One Ltd. v. Hallmark Cards, Inc.[14], a case involving both patent and trade secret issues, the Federal Circuit affirmed a Missouri District Court opinion. The district court held that, under a property theory of trade secrets, once Group One's asserted trade secrets were disclosed in a published Patent Cooperation Treaty (PCT) application, their status as trade secrets was destroyed.[15]

Based on the district court finding, the Federal Circuit affirmed that damages for misappropriation "were limited to any 'head-start' advantage Hallmark obtained by using the trade secrets between the date Group One disclosed them to Hallmark and the data the PCT application was published." [16]

These cases illustrate that a legitimate means of public disclosure (i.e., for a patent application) is not a mitigating factor that prevents the loss of trade secret protection. In addition, these cases also illustrate that a legitimate means of public disclosure does not offset or mitigate the amount recoverable by a trade secret owner when a misappropriator is responsible for the disclosure.

Based on these and other opinions, by extension, a party which inputs another's trade secrets into an LLM context window – potentially leading to disclosure via LLM responses to third-party inquiries – could be held liable for that disclosure and responsible for the lost value to the trade secret owner.

A Dual Threat: Copyright Infringement and Trade Secret Misappropriation

The input of trade secret documents into a context window of an LLM solution may raise implications of both copyright infringement and trade secret misappropriation.

Copyright Liability Implications

Business records containing trade secrets are often also protected by copyrights, which generally offers protection against another's unlicensed reproduction, distribution, or creation of derivative works. When a party enters copyrighted works into a context window of an LLM, the following copyright-related issues may be raised:

Unauthorized Reproduction: Entering text or other materials into the context window of an LLM creates a copy, potentially violating the copyright owner's exclusive right of reproduction.

Creation of Derivative Works: The LLM processes and transforms the work entered into the context window, potentially creating unauthorized derivative works.

Distribution to Third Parties: If the LLM provider uses the copyrighted work for training the LLM or if the processed work becomes available to third parties, this may constitute unauthorized distribution.

While fair use defenses might be raised, courts would likely consider the commercial and potentially competitive nature of the use, the potential harm to the copyright owner, and the substantiality of the portion used – all factors that can weigh against a finding of fair use in the copyright context.

Copyright Damages Implications

A finding of copyright infringement and trade secret misappropriation may result in larger claims for monetary recovery:

Copyright awards can include statutory damages (up to USD 150,000 per work for willful infringement), a copyright owner's actual losses, and an infringer's related profits to the extent they exceed an owner's losses.

Trade secret misappropriation awards can likewise include the owner's actual losses, the defendant's unjust enrichment (avoided costs + profits from sales of accused products), reasonable royalties, and potentially exemplary damages.

Both statutes provide for the recovery of attorney's fees as well as injunctive relief.

This dual liability significantly increases the potential financial consequences for defendants who input trade secret information into LLMs.

Insurance Coverage for LLM-Related Trade Secret Disclosure

Companies facing exposure for trade secret misappropriation through use of LLMs may find potential coverage under commercial general liability (CGL) policies, though specific outcomes will likely depend on policy language and jurisdiction.

Potential Policy Provisions Providing Coverage

Advertising Injury Coverage: Certain Commercial General Liability ("CGL") policies cover "advertising injury," which may result from the disclosure of confidential and proprietary information. CGL policies may define "personal and advertising injury" to include "[o]ral or written publication, in any manner, of material that . . . disparages a person's or organization's goods, products or services." [17] If certain types of trade secrets are disclosed through an LLM solution (e.g., internal competitor assessments and/or internal product comparisons) and subsequently published to third parties, this coverage may be triggered.

Property Damage Coverage: Some property insurance policies define "property damage" to include loss of use of tangible property and/or damage to electronic data. Courts in some jurisdictions have recognized trade secrets as property that can be lost or damaged.

Cyber Liability Coverage: Some insurance policies that cover cyber liability may explicitly cover unauthorized disclosure of confidential information via use of LLMs.

Coverage-Related Issues

Companies seeking insurance coverage for improper LLM-related disclosures of trade secrets should consider the following issues:

Intentional Acts Exclusions: Most policies exclude coverage for intentional acts, which could apply if an employee deliberately discloses trade secrets via an LLM.

Data Exclusions: Some policies contain exclusions for electronic data or information-related claims.

Prior Knowledge Exclusions: Insurers may deny coverage if the insured was aware of the potential disclosure before the policy period.

Notice Requirements: Prompt notice to insurers is typically required when a potential claim arises.

Conclusion

LLMs are a type of AI system that offers unprecedented capabilities for information processing and content creation. They also introduce novel risks to IP owners, particularly concerning the protection of trade secrets. For many organizations, trade secrets represent a critical form of IP. Unlike patents or copyrights, trade secrets derive their value precisely from remaining confidential, and once publicly disclosed, they lose value permanently.

The risk and legal issues presented by LLMs represent a new frontier in IP law. Parallels of prior cases concerning the disclosure of trade secrets through legitimate means – such as patent applications – offer insight as to the issues presented by LLMs. However, the potential scale and exponential speed of public disclosure presented by LLMs magnify the potential losses, potential liability and monetary recovery, and urgency of establishing protective measures.

As LLM solutions continue to evolve, organizations should continue to evaluate the policies and procedures that protect against their related risks.

To explore this article and discover how it could influence your business, please contact:

James E. Malackowski at
james.malackowski@jsheld.com or

Robert McSorley at
robert.mcsorley@jsheld.com or

Sarah Zhu at
sarah.zhu@jsheld.com or

Acknowledgements

James E. Malackowski is the Chief Intellectual Property Officer (CIPO) of J.S. Held and Co-founder of Ocean Tomo, a part of J.S. Held. In 2025, the Licensing Executives Society International (LES) recognized Mr. Malackowski with its highest honor – the LES Gold Medal. In 2022, he was inducted into the IP Hall of Fame and received the Q. Todd Dickinson Award for significant contributions to IP as a business asset. He is only the seventh person honored with both the LES Gold Medal and IP Hall of Fame inclusion. Mr. Malackowski has served as an expert on over one hundred occasions on intellectual property economics, including valuation, royalty, lost profits, price erosion, licensing terms, venture financing, copyright fair use, and injunction equities. He has substantial experience as a Board Director for leading technology corporations, research organizations, and companies with critical brand management issues.

Robert McSorley is a Managing Director in J.S. Held's Intellectual Property Practice. Based in the Chicago office of Ocean Tomo, a part of J.S. Held, Robert has 30 years of experience addressing the economic, financial, and accounting issues concerning commercial litigation. Robert has focused on intellectual property disputes since 1998, and regularly evaluates the measures and amounts of monetary recovery for infringement / misappropriation. He has offered expert testimony in federal courts and in depositions on dozens of occasions, and courts and juries have adopted his opinions and conclusions. A certified public accountant and a licensed attorney, Robert is a member of the Licensing Executive Society, the American Institute of Certified Public Accountants, and the Federal Circuit Bar Association.

Sarah Zhu is a Manager in the Intellectual Property Disputes Financial Expert Testimony practice, working out of the Chicago office of Ocean Tomo, a part of J.S. Held. The practice area quantifies economic damages arising from intellectual property disputes and provides general litigation support. Prior to joining Ocean Tomo, Ms. Zhu interned at a global consulting firm in the Intellectual Property and Financial Accounting Valuation practices, working on expert testimony reports and building models for various cases.

[1] A Beginner's Guide to Large Language Models, A. Chockalingam, A. Patel, S. Verma, T. Yeung, NVIDIA Corporation, 2023.
[2] Id.
[3] From Command Prompt to AI Prompt: Unravelling how Prompts in puts are used by LLMs, V. Chuadhary, July 23, 2023, https://www.linkedin.com/pulse/from-command-prompt-ai-unravelling-how-prompts-inputs-vijay-chaudhary/.
[4] Through patent applications, for example.
[5] OpenAI recently released its GPT-4.5 model, stating that it's their largest and best model for chat yet. https://www.shakudo.io/blog/top-9-large-language-models.
[6] Shakudo, May 1, 2025, https://www.shakudo.io/blog/top-9-large-language-models.
[7] Id.
[8] https://www.wipo.int/en/web/trade-secrets.
[9] https://oceantomo.com/intangible-asset-market-value-study/
[10] Beyond USB Storage Devices: The Increasing Risk of USB-Connected Headsets, Webcams, DataLocker, https://datalocker.com/blog/beyond-usb-storage-devices-the-increasing-risk-of-usb-connected-headsets-webcams/
[11] Id.
[12] Tekmira Pharmaceuticals Corp., et. seq. v. Alnylam Pharmaceuticals, Inc., Superior Court of Massachusetts, Civil Action 11-1010-BLS2.
[13] Plus, the restructure of the collaboration agreement; https://www.sec.gov/Archives/edgar/data/1447028/000117184312004102/newsrelease.htm.
[14] Group One, LTD. v. Hallmark Cards, Inc., 254 F.3d 1041 (Fed. Cir. 2001).
[15] Group One, LTD. v. Hallmark Cards, Inc., 254 F.3d 1041, 1051 (Fed. Cir. 2001).
[16] Group One, LTD. v. Hallmark Cards, Inc., 254 F.3d 1041, 1043 (Fed. Cir. 2001).
[17] Xerox Seeks $15 Million for Losses Incurred from Five Lawsuits. Insurer Says Xerox's Policy Doesn't Cover the Losses, TonerNews.com, 2025; https://tonernews.com/forums/topic/xerox-seeks-15-million-for-losses-incurred-from-five-lawsuits-insurer-says-xeroxs-policy-doesnt-cover-the-losses/

JS HELD

This publication is for educational and general information purposes only. It may contain errors and is provided as is. It is not intended as specific advice, legal, or otherwise. Opinions and views are not necessarily those of J.S. Held or its affiliates and it should not be presumed that J.S. Held subscribes to any particular method, interpretation, or analysis merely because it appears in this publication. We disclaim any representation and/or warranty regarding the accuracy, timeliness, quality, or applicability of any of the contents. You should not act, or fail to act, in reliance on this publication and we disclaim all liability in respect to such actions or failure to act. We assume no responsibility for information contained in this publication and disclaim all liability and damages in respect to such information. This publication is not a substitute for competent legal advice. The content herein may be updated or otherwise modified without notice.

J.S. Held, its affiliates and subsidiaries are not certified public accounting firm(s) and do not provide audit, attest, or any other public accounting services. J.S. Held is not a law firm and does not provide legal advice. Securities offered through PM Securities, LLC, d/b/a Phoenix IB or Ocean Tomo Investments, a part of J.S. Held, member FINRA/SIPC. All rights reserved.