ijamrsd.com
JAMRSD
ISSN: 2583-6404
Journal of Advanced Multidisciplinary Research Studies and Development
Peer Reviewed Referred Journal | Bi-monthly | Open Access

GUARDIANS OF THE INVISIBLE: SAFEGUARDING TRADE SECRETS IN THE DIGITAL AGE OF AI AND CYBER VULNERABILITY

Dr. Nityashree Nadar
Information Technology, S.I.W.S. N.R. Swamy College of Commerce & Smt. Thirumalai College of Science, Wadala Mumbai – 31, India.
Email: nityashreenadar15@gmail.com

Abstract
In today's hyper-connected and technologically advanced world, trade secrets represent a critical yet increasingly fragile component of a company's intellectual property portfolio. With the advent of Artificial Intelligence (AI), cloud computing, remote work infrastructures, and sophisticated cyber threats, the traditional boundaries of confidentiality have significantly blurred. This paper explores the emerging risks, legal challenges, and strategic approaches associated with the protection of trade secrets in the digital era. The research delves into how AI tools, while offering productivity and innovation, can also inadvertently expose sensitive information through data scraping, algorithmic reverse engineering, and unauthorized data inference. It highlights landmark case studies and judicial precedents that demonstrate the evolving nature of digital misappropriation of trade secrets, especially in cross-jurisdictional scenarios. Furthermore, the paper critically evaluates India's current legal framework on trade secret protection, in contrast with international best practices such as the U.S. Defend Trade Secrets Act (DTSA) and the EU Trade Secrets Directive. It proposes actionable strategies including AI-integrated compliance systems, robust employee awareness programs, encryption protocols, and legislative reforms aimed at strengthening trade secret regimes. In an age where data is the new oil and information the most traded currency, ensuring the protection of trade secrets is not just a legal imperative but a strategic necessity. This paper calls for a collaborative approach involving policymakers, technologists, legal experts, and industry leaders to build a resilient ecosystem that can preserve the sanctity of confidential information amidst the disruptions of AI and digital transformation.

Keywords: Trade Secrets, Artificial Intelligence (AI), Cybersecurity, Digital Transformation, Data Protection, Intellectual Property, Algorithmic Reverse Engineering, Cloud Computing, Legal Framework, Defend Trade Secrets Act (DTSA), EU Trade Secrets Directive, India, Compliance Systems, Encryption, Information Security.

► *Corresponding Author: Dr. Nityashree Nadar*

Introduction

Trade secrets, confidential business information that provides economic advantage because it is secret and subject to reasonable efforts to keep it so, remain an indispensable component of firms' intangible assets. Unlike patents, which demand public disclosure, trade secrets offer protection precisely because they remain undisclosed. Yet the conditions that made trade secrecy viable historically are under stress: distributed workforces, multi-tenanted cloud infrastructure, pervasive telemetry from devices, and the deployment of Machine Learning (ML) systems that may themselves encode or reveal proprietary knowledge. Notably, generative Artificial Intelligence

(AI) systems (e.g., Large Language Models (LLMs)) and ML pipelines introduce new mechanisms for unauthorized acquisition: employees or external actors can leak secrets via prompts to hosted models; adversaries can extract model behavior by repeated querying (model extraction); and the outputs of models can be reverse-engineered to approximate proprietary algorithms or datasets [1]–[3].

These technological trends have profound legal and policy implications. Courts are increasingly asked to adjudicate misappropriation claims when the alleged theft involves digital artifacts such as model weights, prompt engineering patterns, training corpora, or derived outputs. Jurisdictions vary in their readiness: the United States relies on the Defend Trade Secrets Act (DTSA) and established common-law doctrines; the European Union has harmonized core principles through the Trade Secrets Directive; and India is in a period of reform, with the Law Commission's 2024 Report No. 289 proposing a sui generis legislative framework [4]–[6]. Each jurisdiction must reconcile trade secrecy with competing social goods, employee mobility, innovation diffusion, and public interest disclosures.

This paper aims to (i) map the contemporary threat landscape to trade secrets generated or processed in AI environments; (ii) review recent literature and policy outputs (2024–2025); (iii) identify legal, technical, and organizational gaps; and (iv) propose integrated solutions aimed at practitioners, technologists, and policymakers. The analysis draws on law-review scholarship, policy reports, technical preprints, and contemporary case law and news reporting to ensure currency.

Literature Survey

Contemporary literature on trade secrets in the age of AI coalesces around technical threats (model extraction, prompt injection), doctrinal analysis (what counts as a secret), comparative legal reform, and organizational practice. The following review synthesizes works from 2023–2025 that are most salient to the problem.

AI and Technical Vectors of Risk

Generative models and large pre-trained networks create two related risk categories: (a) active extraction, where adversaries query a model repeatedly, reconstructing aspects of training data or model behavior (model extraction and distillation), and (b) passive leakage, where sensitive information is unintentionally exposed through model responses, logs, or telemetry. Recent technical analyses document how model outputs can be probed to recover memorized training data or to approximate proprietary routines, a process that can be weaponized by competitors or malicious actors [1], [3]. Prompt injection attacks and jailbreaks, whereby user inputs manipulate model behavior or coax disclosures, have been empirically demonstrated across multiple platforms and are catalogued in security advisories such as OWASP's GenAI project [7] and recent arXiv analyses [3]. These vulnerabilities are particularly acute in enterprise deployments where employees may supply proprietary prompts to third-party APIs or use public instances of LLMs for work tasks, thereby risking exfiltration and third-party retention of confidential inputs [1], [3], [7].

Legal Scholarship: Recalibrating Doctrines for AI

Legal scholars have examined how trade secret law must adapt to AI-driven contexts. Sprankling's analysis considers whether AI-generated information warrants trade secret protection and how doctrines like "readily ascertainable" or independent creation should be recalibrated when AI capabilities change what is discoverable [2]. Hrdy highlights the specific risk generative AI poses when employees or contractors divulge proprietary information to cloud-hosted AI services,

raising the bar for "reasonable measures" a secret owner must take [1]. These works argue that while core triadic criteria, secrecy, economic value, and reasonable efforts, remain central, their operationalization must account for the ease of replication and inference enabled by modern models.

Comparative Law and Policy

Comparative literature emphasizes divergence and convergence across jurisdictions. The EU's Trade Secrets Directive (2016) establishes a three-part test for trade secret status and sets rules on lawful acquisition, but member states implement and interpret standards with variance [5], [8]. The United States supplements common law with the DTSA (2016), enabling federal civil actions and codifying certain remedies. India historically relies on contract law, equitable doctrines (breach of confidence), and tort remedies; however, the 2024 Law Commission Report No. 289 and its draft Trade Secrets Bill signaled an intention to create a statutory framework tailored to India's needs [6], [12]. Policy analyses stress that statutory clarity (definitions, remedies, interim relief) will be crucial for enforcement in digital contexts.

Litigation and Empirical Trends

Empirical legal and media reporting indicate an uptick in trade secret litigation involving AI and software. High-stakes verdicts and settlements in 2024–2025 show courts willing to award substantial damages and injunctive relief in technology cases where misappropriation is proven; recent reporting of large awards underscores the economic stakes involved [9]. Meanwhile, industry disclosures (e.g., OpenAI's public statements about suspected model distillation attempts by other parties) and journalistic exposés on prompt injection vulnerabilities highlight practical risks to corporate secrets [10], [11].

Organizational and Governance Studies

Policy and business literature recommend governance mechanisms: data classification, least privilege access, AI usage policies, logging and monitoring of prompts, contractual safeguards with cloud providers, and workforce training. These measures are frequently advocated as baseline controls to satisfy the "reasonable efforts" prong that courts examine when assessing trade secret status [1], [6], [12].

Findings

Synthesizing the technical literature, legal analyses, and current events yields five principal findings, which are discussed in detail in next section.

Generative AI and Related Techniques Are Material Vectors for Misappropriation

Generative AI changes both the ease and modes of acquiring proprietary knowledge. Prompt submission of confidential materials to hosted LLMs, model extraction via adversarial querying, and knowledge distillation allow third parties to reconstruct or approximate trade-secret assets without classical theft or physical intrusion. Recent technical reports and security advisories demonstrate that prompt injection and model memorization are practical risks in production systems [3], [7], [11].

Traditional Doctrines Are Stress-Tested but Not Obsolete

The three-part definition of trade secrets (secret, commercial value, reasonable protection) remains analytically useful, but courts and regulators face new questions in applying these elements to algorithmic artifacts, model weights, prompts, and derived datasets. Issues such as whether model behavior or outputs constitute "information" that can be secretable are active topics in academic debate [1], [2].

Jurisdictional Fragmentation Generates Enforcement Gaps

Cross-border data flows and cloud deployments complicate choice-of-law and enforcement. A secret hosted on servers in one country, accessed by employees globally, creates multiple potential jurisdictions and regulatory regimes. India's proposed reforms would create a statutory basis for redress domestically, but cross-border enforcement will still require international cooperation [6], [8].

Procedural and Evidentiary Challenges Are Heightened

Proving misappropriation where the alleged copying occurs via borderline lawful activities (e.g., scraping, Application Programming Interface (API) queries) or where the competitor claims independent model development makes evidentiary burdens heavier. Furthermore, litigation itself risks disclosing sealed information unless procedural protections (sealing, in-camera review) are robust and efficiently applied [6], [12].

Organizational Practices Lag Scientifically Demonstrated Risks

SMEs and many larger enterprises still lack formal policies addressing AI usage, prompting, and model hosting. Where organizations do not implement data classification, prompt governance, and contractual protections with vendors, courts may find insufficient "reasonable steps" to maintain secrecy, weakening legal protections [1], [6].

Issues and Challenges

The modern trade secret landscape is shaped by interlocking legal, technical, and organizational challenges. This section catalogs the key issues and explains their significance.

Definitional Ambiguity and the "Readily Ascertainable" Problem

Courts must decide whether information that can be inferred from public observations (via AI) should still count as secret. The doctrine of "readily ascertainable" historically shields information discoverable through reverse engineering or public inspection; now, AI-based inference may make previously secret information computationally recoverable. Some commentators argue this requires raising the bar for secrecy or rethinking "readily ascertainable" to consider probabilistic inference [2].

Model Extraction, Distillation and Reverse Engineering

Technically, repeated queries can reconstruct model decision boundaries or generate distilled models that replicate functionality. Distillation can be innocuous, but when based on proprietary outputs or training sets it can substitute for direct acquisition. Distinguishing legitimate re-implementation from unlawful appropriation is non-trivial, especially when the recreated artifact is functionally similar but not verbatim [1], [5].

Prompt Injection and Telemetry Leakage

Prompt injection attacks can cause models to divulge confidential content present in system prompts or cached context. Furthermore, using third-party APIs without contractual data protections can result in prompt logs being retained and reused in model updates, thereby leaking proprietary inputs [3], [7], [11]. Regulatory frameworks currently lack uniform standards for API providers' handling of customer prompts.

Litigation Risks and Exposure During Discovery

Trade secret litigation often requires some disclosure of the secret to the court and opposing counsel. Without reliable sealing procedures, security protocols, and expedited hearings, the owner may risk permanent disclosure. India's existing case law offers equitable remedies but lacks comprehensive procedural mechanisms; the Law Commission's draft contemplates confidentiality orders but implementing effective in-camera processes remains a practical challenge [6], [12].

Employee Behavior, Third-Party Services, and Contractual Shortcomings

Employees using public LLMs or cloud storage, or contractors who mishandle data, are primary vectors. Contracts with cloud vendors may contain ambiguous or weak data usage and retention clauses. Where data governance fails, courts may deem trade secrets insufficiently protected. Conversely, overly broad NDAs or non-compete clauses can provoke statutory or policy resistance and may be struck down for restraint of trade.

International Enforcement and Attribution Problems

When a foreign entity uses extracted model outputs to compete, domestic remedies may be economically hollow unless cross-border enforcement is practicable. Attribution is also difficult in ML contexts—linking a model's behavior to a specific prior secret requires careful technical and expert evidence, which raises costs and complexity.

Balancing Public Interest and Whistleblowing

Trade secret laws must protect legitimate confidentiality without unduly suppressing disclosures in the public interest (e.g., health or safety violations). Whistleblower protections should be calibrated to allow reporting while protecting innocent trade secret holders; statutory frameworks sometimes struggle to thread this needle.

Solutions for the Current Issues and Challenges

Addressing this multi-dimensional problem requires legal reform, technical controls, contractual strategies, governance, and international collaboration. Below is a practical, prioritized framework that integrates these dimensions.

Legal & Policy Reforms

Codify Clear Definitions and Remedies

Jurisdictions should adopt statutory definitions that clearly identify (i) what classes of AI artifacts and outputs can be trade secrets (e.g., model weights, proprietary prompts, curated training datasets, pipelines), and (ii) examples of misappropriation that include model extraction, prompt scrapes, and unauthorized inference. India's Law Commission Report No. 289 provides a draft template for such a statute; it should be enacted with careful drafting to ensure clarity on defences (reverse engineering, independent creation, public interest) [6].

Strengthen Procedural Tools

Legislation should permit sealed filings, in-camera review, restricted access to sensitive discovery, expedited injunctive relief, and protocols for protective orders tailored to digital artifacts. Courts should adopt special procedures for handling machine-readable evidence and expert technical affidavits to avoid unnecessary disclosure.

Calibrate Criminal and Civil Sanctions

Effective deterrence requires meaningful civil remedies (damages, disgorgement, permanent injunctions where appropriate) and criminal sanctions for egregious economic espionage. The DTSA model can inform civil remedies; criminal law should be narrowly tailored to intentional, malicious conduct.

Whistleblower and Compelled Disclosure Safeguards

Statutes must embed safe harbors for whistleblowers and carveouts for disclosures required by law (e.g., to regulators or for public health), with confidentiality protections and limited scope.

Technical Controls & Security Engineering

Data Classification and Least Privilege

Organizations must classify data by sensitivity and enforce least privilege access, ensuring that only authorized entities can query or retrieve secrets. AI systems should integrate data-aware admission controls so that sensitive inputs are blocked from third-party APIs [1], [3].

Prompt Governance and Prompt Logging Controls

Enterprises should adopt policies forbidding upload of secrets to public LLMs, use private or on-premise models for sensitive tasks, and maintain secure, encrypted logs with strict access control. Where third-party APIs are used, contracts must specify retention, reuse, and deletion policies for prompts and outputs.

Differential Privacy, Watermarking, and Fingerprinting

Use differential privacy techniques when training models on proprietary data to reduce memorization risk, and incorporate watermarks or cryptographic fingerprints in outputs or datasets to support attribution if leakage occurs.

Adversarial Robustness & Monitoring

Regular red-teaming to detect prompt injection vulnerabilities, rate limits to impede extraction attacks, anomaly detection for suspicious query patterns, and continuous monitoring of model outputs can reduce risk. Security advisories such as OWASP's guidance are practical starting points [7], [3].

Secure Development and Deployment Practices

CI/CD pipelines should include secrets scanning, ephemeral credentials, encrypted secrets stores (e.g., hardware security modules), and strict network segmentation between development and production.

Contractual and Commercial Measures

Vendor Contractual Clauses

Contracts with cloud providers and AI-service vendors must address intellectual property protections explicitly: prohibit training on customer data without consent, require prompt deletion on termination, and provide audit rights. Where vendors are unwilling to offer acceptable terms, organizations should prefer private hosting or self-hosted models.

Employee Agreements and Policies

Update NDAs, offer letters, and acceptable-use policies to address AI limitations and explicit prohibitions on uploading confidential information to external models. Ensure policies are narrowly tailored to be enforceable and compliant with labor law.

Insurance and Incident Response

Cyber-insurance products are evolving to cover AI-related incident response. Maintain documented incident response plans that include steps for suspected trade secret leakage: forensic preservation, legal hold, rapid injunctive relief, and remediation.

Organizational Culture, Training, and Audits

Continuous Training

Implement recurring training for employees and contractors that explains what trade secrets are, practical examples, and explicit guidance on AI tool use. Use simulated exercises that show how prompt submission may leak confidential input.

Executive Oversight

Boards and senior executives should receive briefings on AI risk and trade secret exposure, and include trade secret risk metrics in enterprise risk assessments.

Third-Party Due Diligence

Vet partners, suppliers, and M&A targets for their data governance practices. Include trade secret risk as part of contractual warranties and indemnities in commercial transactions.

Litigation Strategy & Evidence Handling

Early Preservation and Forensics

At the first sign of misappropriation, preserve logs, model snapshots, and relevant network records. Engage technical experts to analyze model behavior and correlate artifacts to the alleged secret.

Protective Orders and Sealing

Move promptly for protective orders that limit disclosure during discovery and request in-camera review when necessary. Draft pleadings to avoid exposing the substance of secrets while adequately notifying the court of the harm.

Technical Expert Testimony

Use expert witnesses capable of explaining model extraction and demonstrating via controlled experiments how similarity or copying occurred, including statistical measures of overlap.

International Cooperation and Standards

Harmonization of Core Principles

Encourage convergence around baseline definitions and procedural norms (e.g., "reasonable steps," lawful acquisition). Multilateral fora and standard-setting bodies (e.g., WIPO, OECD) can help reduce enforcement friction.

Cross-Border Mutual Assistance

Create mechanisms for expedited preservation orders and cross-border discovery when misappropriation involves cloud services and foreign actors.

Industry Standards and Certification

Develop industry certifications for "AI-secure" service providers that meet minimum contractual and technical requirements regarding training data usage and prompt privacy.

Conclusion

Trade secrets are increasingly at risk in a world where AI systems can both synthesize and reveal proprietary knowledge. The digital transformation that empowers innovation also expands attack surfaces: prompt injection, model extraction, and inadvertent employee disclosures to cloud services are concrete threats that demand a coherent response. The literature from 2024–2025 underscores the urgency: legal doctrines are being reexamined, policymakers are proposing statutory reforms, and technical research documents vulnerabilities and mitigation strategies. A durable defense requires a tripartite approach. First, legal reform must provide clarity on what constitutes trade secrets in AI contexts and offers robust procedural protections for confidential evidence. Second, technical controls must be embedded into organizational systems: security-first AI development, prompt governance, logging, watermarking, and privacy-preserving training. Third, organizational governance—worker training, contractual discipline with vendors, and board-level attention—will operationalize legal and technical measures. International cooperation and harmonized standards will further reduce the friction of enforcing rights across borders. India is at a critical juncture: the Law Commission's Report No. 289 and the proposed Trade Secrets

Bill provide a template to create a statutory backbone for protection [6]. If enacted thoughtfully and paired with resources for enforcement and technical capacity building—especially for SMEs—India can balance economic dynamism and protection of confidential innovation. Ultimately, protecting trade secrets in the digital age is not merely a legal endeavor; it is a strategic business requirement and a socio-technical challenge. By aligning law, engineering, and governance, stakeholders can preserve the "invisible" assets that underpin competitive innovation while ensuring necessary public safeguards. The task is urgent: as AI matures and pervades industries, the time to fortify the guardians of the invisible is now.

References

1. C. A. Hrdy, "Trade Secrecy Meets Generative AI," Chicago-Kent Law Review (Kent Law Scholarship),Jan. 31, 2025.
Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5121745
2. J. G. Sprankling, "Trade secrets in the artificial intelligence era," SSRN Electronic Journal, 2024.
Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4847813
3. "Multimodal Prompt Injection Attacks: Risks and Defenses," arXiv preprint, Sep. 2025. Available: https://arxiv.org/abs/2509.05883
4. EUIPO, "Trade secrets: Vital intellectual property assets," EU Intellectual Property Office, May 16, 2024. Available: https://www.euipo.europa.eu
5. WIPO, "Trade Secrets — Country Overviews & EU Directive Summary," WIPO Comparative Analyses, 2024. Available: https://www.wipo.int
6. Law Commission of India, "Trade Secrets and Economic Espionage — Report No. 289," Mar. 2024.
Available:https://cdnbbsr.s3waas.gov.in/s3ca0daec69b5adc880fb464895726dbdf/uploads/2024/03/2024030619823188 41.pdf
7. OWASP GenAI Security Project, "LLM01:2025 Prompt Injection," Open Web Application Security Project, 2025. Available: https://genai.owasp.org/llmrisk/llm01-prompt-injection/
8. European Commission / Member State Guidance on the Trade Secrets Directive, WIPO country sheet (EU overview), 2024.
Available:https://www.wipo.int/documents/d/trade-secrets/docs-overview-country-sheets-eu-final.pdf
9. Reuters, "Trade secret misappropriation: permanent injunction and monetary damages," Jun. 13, 2025. (Coverage of Insulet Corp. v. EOFlow Co. verdict and damages). Available: https://www.reuters.com/legal/legalindustry/trade-secret-misappropriation-permanent-injunction-monetary-damages-2025-06-13/
10. Financial Times, "OpenAI says it has evidence China's DeepSeek used its model to train competitor," Feb. 2025. Available: https://www.ft.com/content/a0dfedd1-5255-4fa9-8ccc-1fe01de87ea6
11. The Guardian, "ChatGPT search tool vulnerable to manipulation and deception, tests show," Dec. 24, 2024.
Available: https://www.theguardian.com/technology/2024/dec/24/chatgpt-search-tool-vulnerable-to-manipulation-and-deception-tests-show
12. SpicyIP, "Law Commission's 289th report — Trade Secret and Economic Espionage," May 15, 2024. Analysis and commentary on India's policy proposals. Available:

https://spicyip.com/2024/05/law-commissions-289th-report-trade-secret-and-economic-espionage.html
13. "Knowledge Distillation and IP Concerns," Proceedings of the Intellectual Property Researchers of Europe Conference, Geneva, Jun. 2025 (SSRN preprint), available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5348009
14. CRA International, "Trade Secret Litigation Watch: August 2025," Aug. 22, 2025 (trend summary and litigation statistics). Available: https://www.crai.com/insights-events/publications/trade-secret-litigation-watch-august-2025/