akerman

Blog Post

AI-Enhanced Misappropriation: When Departing Employees Leave with More Than Just Client Lists

June 9, 2026

By M. Adil Yaqoob

Consider the scenario: a higher-up employee uploads six months of internal strategy documents into a generative AI tool, generates a ten-page competitive playbook synthesizing the company's pricing models, customer relationships, and go-to-market plans, and resigns the next morning. Nothing was forwarded, downloaded, or copied in the traditional sense—but the employer's most valuable information just walked out the door in a new form.

Artificial intelligence has rapidly transformed workplace productivity. Employees now routinely use generative AI tools to summarize documents, organize information, draft communications, and analyze large datasets. But those same tools are also creating new trade secret, confidentiality, data security, and restrictive covenant risks that many employers have yet to confront.

Prior Akerman guidance has addressed general workplace AI use and confidentiality risks, and related Akerman guidance on AI in hiring has explored the regulatory landscape for AI-driven employment decisions. The higher-stakes scenario arises when those risks converge with employee departures, competitive moves, and trade secret litigation.

Related People

M. Adil Yaqoob

Related Work

Employment Litigation
Employment Training and Compliance
Labor and Employment
Trade Secrets, Restrictive Covenants, and Unfair Competition

Related Offices

New York

HR Defense

Akerman Perspectives on the Latest Developments in Labor and Employment Law

Visit this Akerman blog

Historically, employers worried about departing employees leaving with client contacts, pricing spreadsheets, source code, confidential presentations, or strategic plans. Today, the concern is broader. Employees can use AI tools to rapidly synthesize large volumes of proprietary business information into portable summaries, strategic playbooks, customer analyses, code libraries, pricing insights, or competitive intelligence before walking out the door.

As a result, employers increasingly face a difficult question: did the employee merely rely on general skill, knowledge, and experience, or did the employee use AI to extract, transform, or repackage confidential information in a way that may support trade secret, confidentiality, computer access, or restrictive covenant claims? That question has a corollary that remains largely unresolved: when AI tools used during employment blur the boundary between personal skill and company information, what can a departing employee legitimately take with them? This article focuses on the employer's perspective, but that unresolved tension will shape the development of this area of law.

AI Changes the Nature of Information Extraction

Traditional trade secret disputes often involved employees forwarding documents to personal email accounts, downloading files onto external drives, or copying materials to cloud storage. Those scenarios remain important, but generative AI introduces a different kind of risk.

Now employees may upload internal documents into a third-party AI system and generate outputs based on source material. The outputs may not resemble the source material at all, but they may nonetheless be derived from it. This creates a significant evidentiary challenge: when AI transforms trade secrets into summaries, syntheses, or process redesigns that bear no textual resemblance to the

source material, traditional litigation strategies that rely on word-for-word comparison to prove misappropriation may be insufficient.

That distinction matters. The key legal question is not whether the output resembles the original file but whether it was derived from protectable confidential or trade secret information and whether the employee acquired, used, retained, or disclosed that information in a manner prohibited by law, contract, or company policy. Courts have not yet directly addressed whether AI-generated summaries of trade secrets constitute misappropriation of the underlying secrets, but the direction of the law strongly suggests that derivation—not duplication—is the operative inquiry.

AI use does not automatically establish wrongdoing. Employers still must prove the traditional elements of their claims, including that the information was protectable, that the employer took reasonable measures to maintain its secrecy, and that the employee improperly acquired, used, disclosed, or threatened to use it. AI may strengthen the factual narrative, but it does not eliminate those requirements.

Metadata and Forensics Now Matter More Than Ever

Employers investigating suspicious departures are discovering that traditional forensic methods may not fully capture AI-related activity. Conventional reviews often focus on email forwarding, USB transfers, cloud-storage uploads, file downloads, printing logs, and access patterns on shared drives. Those sources remain important, but generative AI tools often leave a different kind of trail.

Depending on how an employer's systems are configured—including endpoint monitoring software, which tracks activity on individual devices; data loss prevention tools; browser telemetry, which records web activity and data

flows; and device-management platforms—potential indicators may include browser histories reflecting AI platform usage, unusually large clipboard activity, mass copying of internal text into browser sessions, AI-generated summaries stored locally, deleted temporary files, anomalous access to repositories shortly before resignation, or files created shortly after large volumes of confidential information were accessed.

Even where such evidence exists, it may not answer every question. Browser history may show that an employee visited an AI platform, but not necessarily what was pasted, uploaded, generated, downloaded, or retained. Personal AI accounts may be outside the employer's direct control, and enterprise AI logs may depend on the platform, configuration, and contractual terms.

Forensic review should be coordinated carefully with legal obligations. Once litigation is reasonably anticipated, employers should preserve potentially relevant prompts, outputs, chat histories, browser artifacts, SaaS logs (activity records maintained by cloud-based software providers), device images, and account records. Employers should avoid directing employees to delete potentially relevant AI-generated materials before preservation obligations have been evaluated.

Existing Policies May No Longer Be Sufficient

Many confidentiality, acceptable-use, bring-your-own-device (BYOD), and information-security policies were drafted before widespread enterprise AI adoption. As a result, employers may prohibit disclosure of confidential information in general terms without addressing how employees interact with AI systems, a gap that is becoming harder to ignore.

That gap can matter. Employers seeking injunctive relief often benefit from showing that they took reasonable measures to protect confidential

information. The absence of an AI-specific policy will not necessarily defeat trade secret protection, but it may complicate the employer's ability to show that it addressed foreseeable methods of disclosure or misuse.

Employers should consider whether existing policies adequately address uploading company information into generative AI tools, using personal AI accounts for work-related tasks, summarizing internal documents through AI platforms, storing or forwarding AI-generated outputs, using AI tools to analyze customer or pricing data, and retaining AI-generated derivative materials after employment ends.

Policies should also define ownership and control of AI-generated work product created for business purposes and define confidential information broadly enough to cover extracts, summaries, analyses, prompts, outputs, embeddings, derivative materials, and other AI-assisted transformations of company information. At the same time, policy updates should preserve legally protected disclosures, whistleblower activity, agency reporting, and employee rights to discuss wages, hours, and working conditions.

Restrictive Covenant Litigation Is Evolving

Employers pursuing restrictive covenant, confidentiality, or trade secret claims are increasingly focused on forensic evidence surrounding employee departures. In many disputes, the timing and scope of data activity now play a central role in temporary restraining order and preliminary injunction proceedings, sometimes as much as the underlying covenant language itself.

Courts may scrutinize whether an employee accessed unusual quantities of information before resigning, used unauthorized AI tools, circumvented company monitoring controls, generated derivative strategic materials shortly before joining a

competitor, or retained AI-generated documents after being asked to return or delete company information.

At the same time, employers should be careful not to overstate what AI evidence proves. AI-related activity may be relevant to misuse, threatened misappropriation, breach of confidentiality obligations, or irreparable harm, but it does not make an otherwise unenforceable restrictive covenant enforceable. Policy clarity, training, and consistent enforcement remain especially important given that many employees use AI tools entirely for legitimate productivity purposes.

Monitoring Must Be Paired with Legal Compliance

AI-related monitoring can be an important component of trade secret protection, but it should not be implemented casually. Monitoring browser activity, clipboard usage, AI tool interactions, SaaS logs, or activity on personal devices and personal accounts may raise issues under privacy laws, electronic monitoring notice requirements, wiretap and stored communications statutes, computer access laws, employee consent rules, and labor-law protections.

For that reason, employers should coordinate monitoring and forensic protocols with legal, IT, HR, and cybersecurity stakeholders. Monitoring programs should be tied to legitimate business purposes, disclosed where required, implemented consistently, and designed to avoid unnecessary collection of personal or protected information. Employers should be especially cautious when an investigation involves personal devices, personal email accounts, personal cloud storage, or personal AI accounts.

Practical Steps Employers Should Consider

As AI usage becomes increasingly embedded in day-to-day operations, employers should consider

proactively revisiting their trade secret protection strategies. That review should include policies, training, technical controls, forensic readiness, vendor management, and exit procedures.

Employers may wish to review confidentiality and acceptable-use policies for AI-related gaps, establish approved enterprise AI platforms, prohibit or limit uploading sensitive information into public AI systems, define permissible and impermissible AI use by data category, implement monitoring protocols for anomalous data activity, conduct targeted exit interviews for high-risk employees, review BYOD and remote-access controls, and coordinate legal, IT, HR, and cybersecurity teams when investigating suspicious departures.

Exit procedures should also be updated for AI-related risks. Employers may consider asking departing employees to certify that they have not uploaded confidential information to unauthorized AI tools, retained AI-generated summaries of company information, stored company prompts or outputs in personal accounts, exported AI platform memories or conversation histories containing company information, or used AI tools to create materials derived from confidential company information. Exit certifications should specifically address whether the employee exported AI memories—conversation histories and contextual information that AI platforms allow users to port between accounts or platforms—containing synthesized proprietary information. Litigation hold and forensic preservation procedures should also be evaluated to determine whether they adequately account for AI-generated content, browser-based activity, SaaS logs, and account histories.

Takeaways

Generative AI is changing how employees interact with information, and the risks associated with employee departures are expanding accordingly. Rather than restating the full scope of these issues,

the following action items represent the most immediate steps employers should take:

First, update AI acceptable-use policies to specifically address uploading confidential information into AI tools, retaining AI-generated outputs, and exporting AI platform memories. Second, add AI-specific questions to exit interviews and certifications, including whether the employee used AI tools to summarize, synthesize, or reorganize company information. Third, coordinate forensic preservation procedures with AI platform vendors to ensure that prompts, outputs, chat histories, and memory exports are captured when litigation is anticipated. Fourth, review whether existing NDAs and confidentiality agreements define protected information broadly enough to cover AI-generated derivative materials.

Employers need not treat every AI-related event as misconduct, but they also should not assume that traditional, pre-AI policies, monitoring practices, and exit procedures remain sufficient for the AI era. Organizations that take the time now to update expectations, preserve relevant evidence, and coordinate their legal and technical response protocols will be better positioned to protect confidential information when these disputes arise.

Employers with questions related to this topic should contact their Akerman Labor & Employment attorney.
