Reverse Engineering in the Age of AI: Are Your Trade Secrets Still Safe?

By: Gregory S. Bombard and A.J. Tibbetts

Artificial intelligence (AI) has dramatically expanded the toolkit available for reverse engineering, and in-house counsel might wish to take note. Reverse engineering is the process of discovering otherwise nonpublic information about a product by examining the public-facing product. Reverse engineering has always presented a risk, but rapidly-evolving technology is expanding the scope of what can be reverse-engineered. Now, AI enables reverse engineering in previously-impossible ways. What once required specialized expertise and significant time investment can now be accomplished in minutes using publicly available AI models. This is a noteworthy development for in-house counsel at companies with technology-driven products and services (both specialized "software as a service" (SaaS) companies and also technology companies generally). Companies should consider whether their confidential information protections are up to the task.

Legal Landscape: Trade Secrets and Reverse Engineering

Recent cases show courts and companies struggling to grapple with the law of reverse engineering in the AI era. As AI systems grow more capable, the tension between "reasonable measures" to protect confidential information and "proper means" of reverse engineering continues to grow.

Trade secret law in the United States is governed primarily by two statutes: the Uniform Trade Secrets Act (UTSA), adopted in some form by 48 states, and the Defend Trade Secrets Act (DTSA), a federal law enacted in 2016. Both define a trade secret as information that derives independent economic value from not being generally known or "readily ascertainable" by others, and that is subject to reasonable efforts to maintain its secrecy. Both statutes are directed at "misappropriation," the act of acquiring or using confidential information by "improper means." Importantly, both the UTSA and DTSA include an express carve out from the concept of "improper means" for "reverse engineering." If a competitor divines otherwise secret information by analyzing a publicly available product, then this does not qualify as misappropriation under these trade secret laws.

The line between proper and improper means is increasingly blurred in the AI era. Courts have previously held that "scraping" data using bots, impersonating users, or injecting malicious prompts into AI systems can constitute "improper means" under trade secret law. In one 2003 case, an early use of software robots to extract proprietary data was deemed misappropriation, despite the lack of explicit usage restrictions on the plaintiff's website. Since that decision, however, AI tools have only become more sophisticated and their usage more widespread and knowledgeable to the average company and average consumer. As modern AI tools more accurately infer proprietary processes underlying public-facing materials, there is also a potentially increased risk that confidential information, including information that might previously have been maintained as a valuable trade secret, may be deemed "readily ascertainable" and thus unavailable for trade secret protection.

Recent Examples

Courts are thus beginning to confront the intersection of AI capabilities and trade secret law, particularly in cases involving reverse engineering, prompt injection, and data scraping. These cases offer insights into how "improper means" is being interpreted in the AI context, and what in-house counsel might consider noting.

In one case from earlier this year, the plaintiff alleged the defendant used "prompt injection" attacks to extract proprietary methods from the plaintiffs' generative AI platform, information the plaintiff claimed is among its most valuable trade secrets. "Prompt injection" is a technique used to manipulate generative AI systems by crafting inputs that might bypass built-in safeguards and elicit unintended or sensitive outputs. The complaint describes the use of impersonation and false credentials to gain access and argues that prompt injection is not a legitimate benchmarking practice but a form of cyberattack.

In a case from last year, the Eleventh Circuit ruled that scraping proprietary data using bots could constitute misappropriation. In that case, the defendants accessed a publicly available insurance quote system and used automated tools to extract millions of data points, which they then used to launch competing services. The court held that although the data was technically accessible to the public, the method of acquisition, automated scraping at scale, qualified as "improper means." This case is relevant for SaaS systems that expose outputs or interfaces to the public, as it suggests that even lawful access may become unlawful depending on the method and intent.

Protecting Confidential Information in the AI Age

To protect trade secrets in the age of AI-enabled reverse engineering, in-house counsel may want to focus on two emerging threats: (1) scraping of SaaS platforms and (2) prompt injection attacks on generative AI systems. These tactics allow third parties to extract proprietary information without direct access to internal systems—and without necessarily violating traditional access controls.

For SaaS platforms and GenAI providers, the potential risk lies in the public-facing nature of the service. If a competitor can use bots to scrape outputs, metadata, or behavioral patterns at scale, they may reconstruct proprietary algorithms or workflows. First, SaaS companies might consider implementing technical safeguards such as rate limiting, CAPTCHA challenges, and bot detection tools. Second, legal protections may be needed, including updated terms of service that explicitly prohibit automated access, scraping, or reverse engineering. These terms ought to be enforceable and visible to users, and violations should be monitored and documented. Prompt injection presents a different challenge, but the strategy to combat it is similar: first, consider implementing technical protections to safeguard against prompt injection, such as sandwiched prompts, or AI-powered filtering and sanitization; and second, attempt to ensure terms of service have clear usage limitations and prohibitions against improper use.

In addition, companies should not forget about the tried-and-true trade secret management techniques available to all companies.

1. Consider limiting access to confidential material, like source code or proprietary R&D materials to those with a business need to know. Monitor access and usage of that information.

2. Companies should consider implementing a trade secret management program and specific policies to protect confidential information. This policy might include the specific reverse-engineering concepts discussed above.

3. Legal may want to review and update confidentiality provisions in employment agreements and in standard third-party NDA templates.

4. Companies should consider whether and how to label documents containing proprietary information.

5. Companies may want to document the above. Remember, trade secret protections are a creature of litigation. Without strong evidence, companies' hard work may not matter when they need to prove "reasonable measures."

6. Set a regular cadence to review and improve these protections. If a company put its trade secret protection plan in place before 2023, then it may not have considered AI at all. Since the technology continues to rapidly evolve, the best practice is to seek to have policies and procedures keep pace.

By combining legal vigilance with technical safeguards and clear internal policies, companies might stay ahead of these threats and preserve the value of their confidential information in an AI-driven world.

Gregory S. Bombard is a trial lawyer whose practice focuses on trade secret litigation and other IP and commercial disputes. Greg represents pharmaceutical, technology, and manufacturing companies in state and federal courts, as well as in arbitration proceedings throughout the United States. He regularly represents both plaintiffs and defendants in trade secret cases and related claims. Greg is a frequent writer and speaker on trade secret law and is the co-author of the book Protecting and Litigating Trade Secrets (2nd Ed.), published by the American Bar Association.