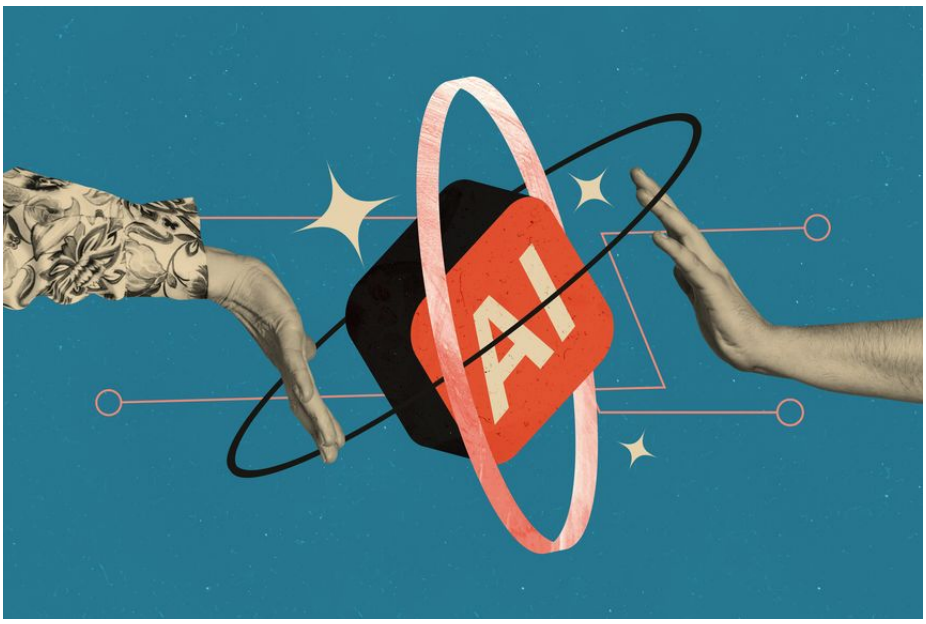
akerman

Akerman Lens

Beyond Training Data: The Hidden Risk of Secondary AI Liability

November 3, 2025

By Samuel T. Kilb and Marc A. Lieberstein



Related People

Samuel T. Kilb
Marc A. Lieberstein

Headlines about AI intellectual property infringement liability tend to focus on direct infringement, i.e., the AI's unauthorized copying/use of others' intellectual property, especially in the context of training data. Somewhat under the radar, however, and potentially riskier for AI providers is the concept of secondary liability: whether the AI provider could be held liable for the actions of those who are using the AI application.

In the classic U.S. context (especially in copyright/infringement cases) the elements of vicarious liability are generally described as: (1) The

defendant has the *right and ability to control* the infringing (or wrongful) activity of the primary actor; and (2) the defendant receives a *direct financial benefit* from the infringing (or wrongful) activity of the primary actor. Some jurisdictions may phrase them slightly differently, but these are the core principles.

For secondary liability in the AI context, the "primary actor" may be the user who uses the AI tool to generate illegal content (copyright infringement, defamation, illegal speech, etc.). The AI company might be secondarily liable if the two elements are satisfied, but because AI tools may autonomously generate or facilitate output, there is some ambiguity: is it the user's act or the tool's? This blurs the control element. Courts have historically limited secondary liability to contexts involving active supervision, but arguments exist that AI providers exercise meaningful control, even if less granular.

With regard to the element of control, factors such as whether the AI company develops and deploys the AI tool, defines terms of service, can moderate/suspend use, can adjust model behavior, or can detect misuse (e.g, for an AI company that offers a generative AI model, it monitors usage logs, sets limits or filters, and/or reserves termination rights) may demonstrate sufficient control. By contrast, broad offline licensing and lack of practical oversight may weaken the control element.

With regard to the element of direct financial benefit, if the AI company profits from the tool (via, for example, subscriptions, ad revenue, or platform fees) and that profit is tied to the volume or nature of the user activity, that may demonstrate sufficient financial benefit to lead to liability. Such a link would need to be driven by the wrongful uses, e.g., the generative model is monetized by charging per-usage and wrongful uses drive more usage. If, however, the wrongful uses are a tiny subset of overall uses and are not monetized or the company

has no way of distinguishing such uses from legitimate uses, the causal link may be weaker.

The financial benefit element may require showing that the company's business model is boosted by the wrongful activity (or that the model implicitly relied on volume of misuse). In some content-platform cases, immunity regimes (e.g., Communications Decency Act § 230) complicate liability for user-generated content, but AI tools may fall into different categories.

Takeaways and Risk Mitigation

- While classic secondary/vicarious liability is somewhat untested in the AI context, the structural features of many AI companies (tool provider + monetization + usage by third parties + ability to control) make it a plausible theory of liability.
- The focus will often be: did the company contribute to the infringing activity/have **sufficient control** and did it receive a **financial benefit** tied to the wrongful use?
- The evolving regulatory environment (especially outside the U.S.) suggests that liability risks for AI companies will increase.
- AI companies should proactively design governance: filtering/monitoring, usage policies, user agreements, transparency, safe-use features, and consider limitations on misuse; obtain permissions via licensing; and consider liability insurance.
- For plaintiffs, the challenge will be tracing misuse, proving company control/benefit, and navigating immunity regimes. For companies, the challenge is to reduce foreseeability of misuse and demonstrate active control/mitigation.

> Unlike human actors, AI lacks subjective intent, political liberties or autonomy in

the legal sense. However, courts and regulators are increasingly faced with cases where AI generated content causes harm or misinformation. The legal frameworks governing agency relationships, vicarious liability and product liability provide useful lenses for examining these issues.

nysba.org/...