LAW.COM

The point isn't that AI companies deserve a free pass or that privacy concerns are imaginary. Many are real. The problem is fit: the legal tools now doing the most work are poorly matched to the harms people actually care about.

May 20, 2026 at 09:00 AM By **Ben Berkowitz**



Ben Berkowitz, with Keker, Van Nest & Peters. Courtesy photo

A California law written in 1967 to stop criminals from tapping telephone lines is now being invoked to sue companies for deploying widely used AI-enabled tools. In the absence of federal legislation, these lawsuits are fast becoming a de facto privacy regime for a growing range of AI-powered technologies. The regulatory vacuum is being filled by judges and juries applying wiretapping statutes to technologies no one could have imagined when those laws were enacted.

I've spent much of my career as a trial lawyer litigating disputes involving emerging technologies, privacy and cybersecurity. I primarily represent technology companies in this litigation, and that perspective informs my view. Still, after watching these cases unfold in courtrooms across the

country, I'm convinced the current moment is failing everyone—including the consumers these suits are supposed to protect.

The point isn't that AI companies deserve a free pass or that privacy concerns are imaginary. Many are real. The problem is fit: the legal tools now doing the most work are poorly matched to the harms people actually care about. The result is litigation that too often delivers little more than pop-up notices and longer privacy policies instead of meaningful privacy protections, while imposing enormous costs and uncertainty on companies trying to build and deploy useful products.

Why This Wave of Litigation Exists

These suits didn't arise in a vacuum. AI systems collect and process personal data in ways that can feel opaque. Many companies are trying to do this right, building privacy protections into product design, but they're doing it without clear rules. Consumers have legitimate questions about what data is collected and retained, how prompts and outputs are stored, and how information might be used downstream. In the absence of a federal framework setting baseline rules, plaintiffs' lawyers have reached for the statutes that are available.

Today's most common litigation tools are state wiretapping and eavesdropping laws, chief among them California's Invasion of Privacy Act (CIPA), enacted in 1967 for an earlier era of communications privacy concerns. CIPA can carry a $5,000 statutory penalty per violation. Under current theories, plaintiffs label common AI-powered tools—transcription, chat, call analytics—as "eavesdropping devices," and the software vendors that provide them as "third-party interceptors." Each customer interaction processed by the tool, they argue, is a separate violation. Multiply $5,000 by a few million calls or clicks and you have breathtaking exposure.

In recent years, plaintiffs have used CIPA and similar statutes to challenge website chat features, session-replay tools, call analytics, transcription services, and other customer-interaction technologies—often on the theory that the software vendor is a third-party eavesdropper. As those tools increasingly incorporate AI, the same litigation theories are becoming a template for disputes over AI-enabled data processing more broadly.

Consider the implications of such exposure for a regional medical provider using AI transcription software to summarize scheduling calls, or a small business deploying an AI chatbot to answer routine customer questions after hours.

CIPA has an important place in privacy law. But when statutes designed for physical interception are repurposed into all-purpose regulation for modern data practices, the results are increasingly detached from the harms the law was meant to address.

The Mismatch

The problem isn't just scale. It's about what these statutes ask courts to decide. Is the software an "eavesdropping device?" Is the vendor a "third party?" Did information move "in transit" in a way that counts as an "interception?" Cases now turn on technical details like how data is routed, stored, or processed that has little to do with whether anyone actually suffered meaningful harm to their privacy.

That isn't a criticism of judges. It's a structural limitation. Courts apply the statutes they're given. Wiretapping laws are built around formal elements—consent, interception, third-party involvement. But the most urgent AI questions are different. They concern how long sensitive data is retained, who can use it and for what purposes, what safeguards protect it at scale, and what limits should apply to training and downstream use.

Litigation that turns on whether a tool technically "intercepts" data "in transit" can push companies to optimize for legal formalism—designing systems to avoid a statutory definition—rather than optimizing for privacy outcomes. That's not a recipe for better protection.

The Questions That Deserve Answers

AI raises hard privacy questions that today's litigation largely sidesteps. The real issue isn't whether data was "intercepted in transit" but rather what limits should apply to use of personal information for AI inputs and outputs. As AI systems become better at drawing sensitive inferences from ordinary data, what limits should apply to how companies collect, combine, and use that information? What transparency and recourse do people deserve when automated systems influence decisions that impact people's lives, for example, in lending, hiring, housing or insurance?

A court interpreting a 1967 wiretapping statute can tell you whether an AI transcription tool is a "third-party interceptor." It can't tell you what disclosures a job applicant is owed when an algorithm ranks resumes, or what guardrails should apply when models infer sensitive traits from seemingly innocuous data. Those are legislative judgments, and Congress should not leave them to be resolved through case-by-case litigation under statutes written for another era.

A Federal Framework—Done Right

A common response is to call for a federal framework with uniform rules. There's an obvious appeal to national standards. But preemption has risks: a federal law can become a ceiling rather than a floor, locking in weaker protections and preventing states from going further.

The case for federal legislation isn't uniformity for its own sake. It's that AI raises issues that genuinely require national answers. A well-designed federal framework could both establish meaningful baseline protections and reduce the incentive to stretch rotary-era wiretapping statutes into the role of AI regulator.

Done right, a framework would include clear, enforceable limits on data practices that matter for AI: minimization and retention rules for sensitive inputs; constraints on using personal data for model training and improvement without meaningful notice and choice; and heightened protections for sensitive inferences about health, finances or other intimate traits. It should include transparency obligations for consequential automated decisions that are understandable and auditable, not just a disclosure that "AI was used." And it should create enforcement mechanisms calibrated to actual privacy harms and risks that are strong enough to deter misconduct, but not so disconnected from reality that they turn technical disputes into disproportionate liability and exposure.

Some conduct should be plainly unlawful, especially the misuse of sensitive data. But the current wave of AI privacy lawsuits is a symptom, not a solution.

The answer isn't to give new technology a free pass, nor is it to rely on outdated statutes and protracted litigation. Until lawmakers build rules designed for AI and modern data systems, a law written for an era of rotary phones will continue to stand in for AI governance. That is not a durable privacy regime. It is a litigation workaround that fails both companies and consumers.

Ben Berkowitz *is a partner at the law firm Keker, Van Nest & Peters in San Francisco, where he handles trials and appeals in complex cases involving emerging technologies.*

Page printed from: https://www.law.com/therecorder/2026/05/20/how-1960s-wiretap-laws-became-ais-de-facto-regulator/

NOT FOR REPRINT

© 2026 ALM Global, LLC, All Rights Reserved. Request academic re-use from www.copyright.com. All other uses, submit a request to asset-and-logo-licensing@alm.com. For more information visit Asset & Logo Licensing.