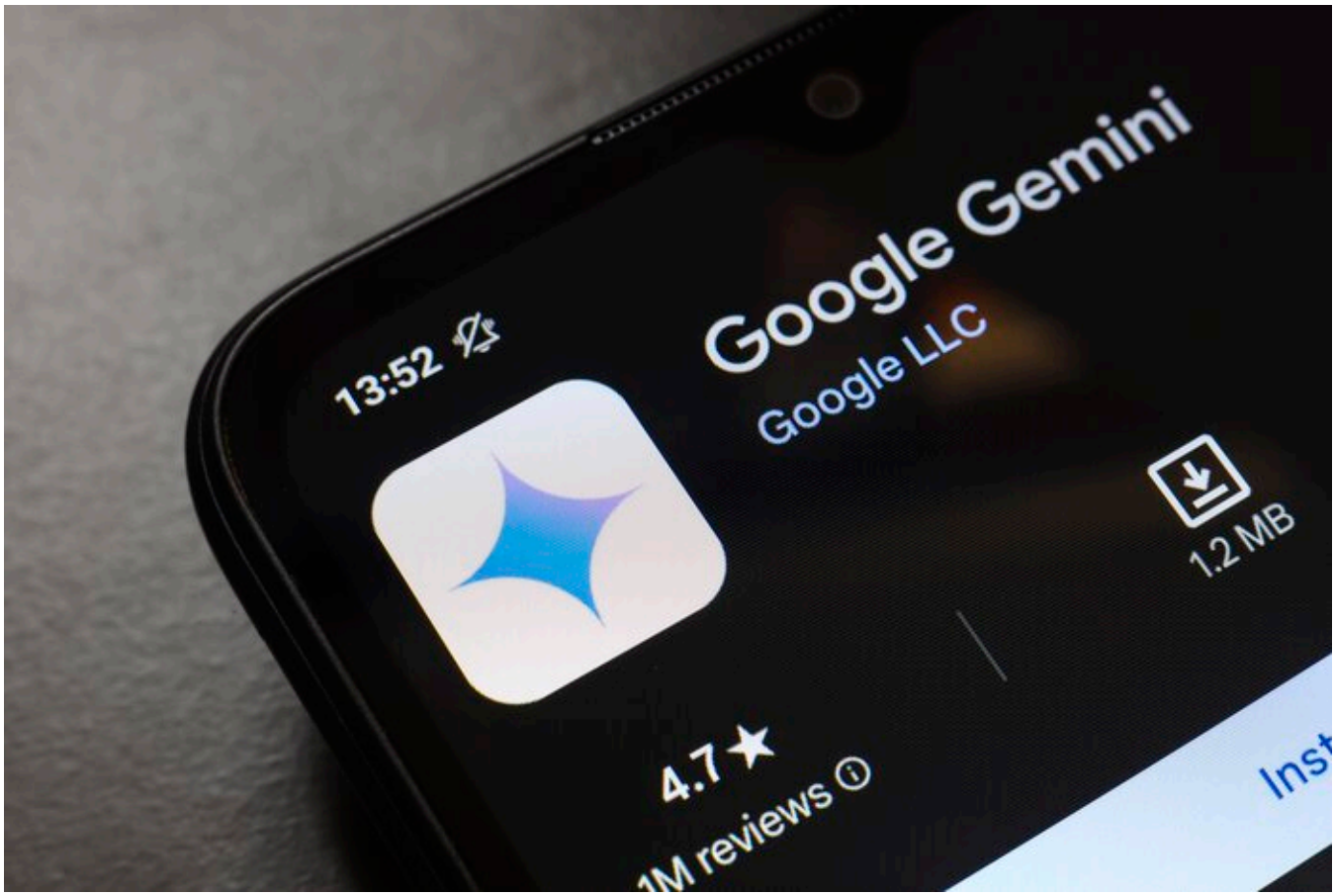
LAW360 Insurance Authority

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Google Suit Reveals Coverage Challenges For AI Integration

By **Abraham Gross**

Law360 (November 20, 2025, 9:12 PM EST) -- A proposed class action brought against Google alleges that the tech giant enabled artificial intelligence tools without disclosing them to users or requesting their consent, highlighting the litigation risks and coverage challenges that can arise when companies integrate AI tools into existing products and services.



A proposed class action in California federal court accuses Google of illegally tracking and storing private communications in its email, chat and videoconferencing services when it secretly enabled its Gemini AI assistant for all users by default. (Photo by Jaque Silva/NurPhoto via AP)

The suit, **lodged in California** federal court Nov. 11, alleges that Google illegally tracked and stored private communications in its email, chat and videoconferencing services when it secretly enabled its Gemini AI assistant for all users by default in October.

For tech experts and counsel representing policyholders, the challenge is just the latest example of a growing body of cases underscoring the potential hazards of AI use — particularly the challenge of integrating AI tools into existing applications.

"'Build first, ask for forgiveness later,' is not an uncommon approach by certain players in the marketplace," said Luke Tenery, head of StoneTurn Group LLP's cybersecurity practice.

The suit brought last week asserted claims for privacy violations under California's Constitution, as well as the Golden State's Invasion of Privacy Act, often dubbed the "wiretapping act," which bars the unauthorized recording or interception of private communications. It also alleged violations of state and federal laws prohibiting intentional access to protected electronic data without consent.

Though the suit targeted Google as an AI developer, similar privacy violation theories are increasingly being applied to companies that deploy third-party AI models, said Matthew Kohel of Saul Ewing LLP, who counsels firms on their use of AI, including AI governance, data privacy, and regulatory and compliance issues.

"These aren't unique to Google, not necessarily unique to AI, but as more companies develop AI tools or implement them, you're going to see, I think, more and more lawsuits, because liability isn't just limited to the developer," he told Law360.

Failing to keep customers apprised of AI integration and use of their data is also a broader issue, as companies see a need to provide information to AI models to improve their performance, Tenery said.

He noted that organizations facing pressure to meet consumer expectations or maintain a competitive edge "may be moving more quickly than regulators can keep up with, or in many cases, the assurances that they can provide consumers, in particular on the protection of their information."

The risks in that approach are magnified by the difficulty in obtaining coverage, said Karin Aldama of Gallagher & Kennedy PA, who represents policyholders.

She noted that cybersecurity policies focus on attacks by outside actors, but enabling an AI that obtains customers' personally identifiable information, or PII, is "a completely different paradigm."

Statutory violations are often excluded from liability policies, as are claims related to disclosures of PII, Aldama said. She added that as AI-related incidents and suits have become more prevalent, AI exclusions have started to appear and will become more common.

"There might be some endorsements developed — I think there probably will be, just because of the widespread use of AI these days — but obviously that will involve extra costs for insurance," she said.

An errors and omissions policy may also have limitations, Aldama said. A licensee of a third party's AI tool can contract around potential privacy issues, but that carries its own potential for a coverage dispute.

"The problem, obviously, is that you have a contract with that party, and so if you're aware that they're using AI, or if you should have been aware that they're using AI, then I can see an insurer argument that this is still intentional conduct and therefore excluded," she said.

Experts compared the current dilemma regarding AI disclosure to suits brought over website tracking cookies, in which plaintiffs have asserted similar privacy and wiretapping claims.

Such suits, which have **posed challenges to coverage**, pushed many companies to disclose their tracking software to customers and allow them to opt out.

Aldama of Gallagher & Kennedy said that in the wake of limited coverage options for AI tools, policyholders should adopt safeguards similar to those they use for cookies: disclose AI tools, the data they collect and whether the data is being used to train the tools, and provide an opt-out.

Privacy claims like those lodged against Google may be less expansive in the future, said Kohel of Saul Ewing, who noted that the California Legislature is still **weighing an amendment** to the California Invasion of Privacy Act that would generally exclude activity with commercial business purposes.

In the meantime, Kohel advised firms to familiarize themselves with their privacy settings and terms of use before providing data to third parties and consider how to provide users with opt-out options, pointing to the Google suit's allegations that the company enabled AI tools without notice.

"That's the heart of the allegation," he said. "Yes, you have the difficulty in opting out as the unintended consequence of third-party data, but it really is about not telling the consumer and giving them the ability to exercise their rights in a meaningful way."

Many AI tools are not as apparent as a chatbot, for example, yet can still process data from customer documents or social media, Kohel said, adding, "The real risk is the embedding of AI tools unbeknownst to users in nonobvious places."

He also suggested that companies push for vendor representations that they anonymize or de-identify the personal information provided to them.

StoneTurn's Tenery said that the common refrain in the critical infrastructure community is "secure by design" or "privacy by design," meaning that customers should craft a comprehensive framework for data privacy and security before implementing new tools.

He said that baking in protections from the outset "has a multiplying effect of assurance," adding that firms that have already made significant AI investments without similarly investing in privacy and security "will be in for a wake-up call."

"I think it's going to be a very difficult truth for many firms to roll that back and/or employ the consent and/or remediation components to regain compliance as these issues arise and mature, from an enforcement and/or regulatory rulemaking standpoint," he added.

--Additional reporting by Allison Grande. Editing by Abbie Sarfo and Nick Petruncio.
