Insights, News & Events

GOOGLE ENGINEER WHO STOLE AI TRADE SECRETS GETS GUILTY VERDICT: LESSONS FOR YOUR BUSINESS

Insights
Feb 9, 2026

Google Engineer Who Stole AI Trade Secrets Gets Guilty Verdict: Lessons for Your Business

A federal jury recently found a former Google engineer guilty on several charges of trade secret theft and economic espionage, in a first-ever conviction of AI-related economic espionage charges. The criminal charges brought by the Department of Justice underscore the serious risks that all companies can face when allowing employees to handle proprietary information and to access trade secrets. And while this case involved allegations that the former engineer stole the information to benefit China, it also shows that the federal government is paying attention to serious instances of trade secret theft. Here's everything you need to know about the conviction and what lessons it can offer your business.

Case Download

The case centers around a former Google software engineer, Linwei Ding, who was indicted on multiple counts for stealing "thousands of pages of confidential information containing Google's trade secrets related to artificial intelligence technology," according to the DOJ.

During an 11-day jury trial in the Northern District of California in January, federal prosecutors presented evidence alleging that while Ding was a Google employee in 2022 and 2023, he used the Apple Notes application on his

Related People

Ron S. Brand
Partner
949.208.8298

Sean Kingston
Partner
949.798.2137

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

work MacBook to create PDF copies of Google's source files. Ding then uploaded them to his personal account, a method that the DOJ says helped him avoid being immediately detected by Google.

During this time, Ding began affiliating himself with two China-based technology companies, and told potential investors "that he could build an AI supercomputer by copying and modifying Google's technology," according to the DOJ. Ding resigned from Google in 2023. The company remotely locked his work laptop and discovered the unauthorized uploads after searching through his network activity history. Google also found that Ding had asked a co-worker to swipe his employee badge to appear as if he was reporting to work in the office.

Federal investigators first brought charges against Ding in early 2024, and he faces a maximum sentence of 10 years in prison for each count of trade secrets theft and 15 years in prison for each count of economic espionage. The DOJ described Ding's activities as putting "US technological leadership and competitiveness at risk."

Protecting Data

Google did take steps to protect its data prior to the breach, practices that were considered "reasonable measures" by the court. Companies are expected to implement basic, good-faith measures to protect proprietary information in order for it to be considered a "trade secret" and legally actionable under the federal Defend Trade Secrets Act (DTSA) and other federal and state laws.

According to court filings, Google required every one of its employees to sign a contract stipulating that:

- Confidential information must be held in "strict confidence";
- Confidential information can only be used for the benefit of Google in the scope of their employment;
- Any documents, materials, or other copies containing confidential information cannot be retained upon termination; and
- Participating in other employment or business activity that directly relates to Google's current, future, or planned

Service Focus

AI, Data, and Analytics

Employee Defection and Trade Secrets

Privacy and Cyber

Industry Focus

Tech

Resource Hubs

AI Governance Hub

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

business, or otherwise conflicts with Google's business interests, is prohibited.

Google employees also were required to sign a code of conduct, which required staff to take steps to protect trade secrets and other confidential intellectual property, and take information security training.

In this case, Ding signed both agreements after he was hired and was also required to sign a Self-Deletion Affidavit after his network activity was flagged by Google.

4 Practical Steps for Employers

There are several steps businesses should consider taking to monitor for potential leaks of trade secrets or other proprietary information:

1. Audit your company's intellectual property. Identify what company information should be considered "confidential" or a "trade secret." This includes labeling and cataloging confidential data and information, such as algorithms, source code, product specifications, service methodologies, pricing, and customer information. Once you've narrowed down these assets, you should clearly label and prioritize these materials based on their sensitivity and limit access to them.

2. Take digital and physical precautions to help monitor network activity and data access. This may include limiting access based on job function and securing data with multi-factor authentication, VPNs, and encrypted servers. Data loss prevention (DLP) tools can also help detect large downloads, external device use, or unusual emailing of code or data. Key physical precautions include locked cabinets/rooms, security badges, employing security staff, surveillance cameras, visitor logs, and/or secure destruction of documents containing protected information.

3. Ensure employees are aware of your company's policies and their obligations to protect sensitive information. Be sure policies address access to, storage of, and appropriate use of proprietary data and trade secret information. Consider requiring nondisclosure agreements (NDAs) or confidentiality and inventions assignment agreements for employees, contractors, vendors, and investors before sharing sensitive data, which include explicit handling requirements and post-engagement non-use obligations.

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

Include confidentiality rules and data sharing practices in employee handbooks, codes of conduct, and employee training materials. Require certifications at offboarding to confirm the return of proprietary materials and post-employment confidentiality obligations.

4. Contact legal counsel if you are concerned about a breach. Federal enforcement agencies have also shown an appetite to investigate these types of crimes in recent press statements.

Identifying leaks in a timely manner can be critical to mitigating the potential damage to your company.

Conclusion

For support in selecting the most appropriate strategy for your business, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Privacy and Cyber Practice Group, Employee Defection and Trade Secrets Practice Group, or Technology Industry Team. Make sure you are subscribed to Fisher Phillips' Insight System to receive the most up-to-date information directly to your inbox.

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.