Testimony before the U.S. House Committee on the Judiciary

Subcommittee on Courts, Intellectual Property,
Artificial Intelligence, and the Internet

Hearing on

# Protecting our Edge: Trade Secrets and the Global AI Arms Race

May 7, 2025

John Villasenor
Professor of Law, Electrical Engineering, and Public Policy
Faculty Co-Director, UCLA Institute for Technology, Law, and Policy
University of California, Los Angeles

Chairman Jordan, Ranking Member Raskin, Chairman Issa, Ranking Member Johnson, Members of the Subcommittee: Thank you for the opportunity to testify at today's hearing.

I am on the faculty of the UCLA schools of law, engineering, and public affairs. I also founded and am faculty co-director of the UCLA Institute for Technology, Law, and Policy. In testifying today, I am providing my own views, and am not speaking on behalf of any institution I am affiliated with. Key points in my testimony include the following:

- Trade secrets are central to American AI leadership
- AI is much more than generative AI
- "Open" AI models still involve trade secrets
- Overly broad AI reporting regulations would open the door to economic espionage
- Overly expansive AI transparency rules would undermine U.S. AI leadership
- The global AI regulation context raises additional trade secret challenges
- Corporate trade secret overreach can impede competition
- AI raises novel trade secret questions
- Fear-based regulation would undermine U.S. AI leadership

## Trade Secrets Are Central to American AI Leadership

America is the clear global leader in AI, a technology that is foundational to our continued economic prosperity and national security. Trade secrets are a vital pillar of U.S. AI pre-

eminence, ensuring that American companies investing to develop new AI solutions have a fair chance to compete in the marketplace.

The competitive differentiation that is so instrumental to the success of the U.S. AI industry is vulnerable in several ways. First, precisely because American AI companies are so innovative and market-leading, they are ripe targets for trade secret theft. Second, policy discussions regarding AI regulation often give insufficient consideration to the potential collateral damage to trade secret rights.

To explore these issues in more depth, I will first provide some background regarding AI and trade secrets generally. I will then address economic espionage, transparency, and the unique trade secret questions raised by AI. I will also provide some more general comments on promoting a regulatory climate that will maintain American AI leadership.[1]

## AI Is Much More than Generative AI

Generative AI, which refers to "deep-learning models that can generate high-quality text, images, and other content based on the data they were trained on,"[2] has attracted enormous attention from policymakers and the broader public in recent years. This attention is justified. The capabilities of generative AI are indeed extraordinary, with profound impacts in areas including the labor market and education.

As remarkable as generative AI is, it is only one part of a broader AI landscape where the advances are equally impressive. In 2024 a pair of researchers from Google DeepMind received a Nobel Prize in Chemistry for their work on AlphaFold2, an AI model that allowed them "to predict the structure of virtually all the 200 million proteins that researchers have identified."[3] This opens the door to discovering new disease-curing drugs that would have been impossible to identify without AI.

AI is also at the core of the algorithms that enable autonomous vehicles to navigate complex city streets. Collaboration between humans and AI is promising to bring improvements to

---

[1] Portions of my written testimony are adapted from John Villasenor, *Artificial Intelligence, Trade Secrets, and the Challenge of Transparency*, 25 N.C. J.L. & TECH. 495 (2024).

[2] Kim Martineau, *What is Generative AI?*, IBM (Apr. 20, 2023), https://research.ibm.com/blog/what-is-generative-AI.

[3] *Press Release*, NOBEL PRIZE (Oct. 9, 2024), https://www.nobelprize.org/prizes/chemistry/2024/press-release/ (awarding two Google DeepMind researchers, Demis Hassabis and John Jumper, one half of the 2024 Nobel Prize in Chemistry; the other half was awarded to David Baker of the University of Washington and Howard Hughes Medical Institute).

medical image interpretation.[4] AI can expand the human capacity to create new inventions,[5] and will revolutionize logistics,[6] weather forecasting,[7] and many other fields. And, AI-powered cyberdefense will be the only effective way to counter a future AI-enabled cyberattack launched on U.S. infrastructure by a geopolitical adversary.

The upshot is that the AI ecosystem is extremely diverse. Put simply, in any domain where computers are used—and in some domains where computers have not traditionally been used—there is the potential to enhance performance using AI. This widespread impact helps explain why there is no one-size-fits-all policy approach that will be suited to all of the many sectors and applications where AI will be used.

What *is* common across all applications of AI is the tremendous opportunity for innovation. In order for the United States to maintain and grow its leadership in AI, developers of AI solutions will need an innovation-friendly business and regulatory climate. With respect to trade secrets, this means ensuring that American AI companies are able to effectively use trade secrets to protect their investments in creating beneficial products and services. At the same time, a healthy innovation climate must also provide checks and balances against overly broad assertions of trade secret rights, which could chill the marketplace by impeding would-be entrepreneurs from leaving established AI businesses to start their own companies.

## A Brief Overview of Federal and State Trade Secret Laws

Under federal law, a trade secret is defined as

> *all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—*

---

[4] Mingyang Chen et al., *Impact of Human and Artificial Intelligence Collaboration on Workload Reduction in Medical Image Interpretation*, 7 NPJ DIGIT. MED. 349 (2024), https://www.nature.com/articles/s41746-024-01328-w.

[5] John Villasenor, *Reconceptualizing Conception: Making Room for Artificial Intelligence Inventions*, 39 SANTA CLARA HIGH TECH. L.J. 197 (2023).

[6] Kristin Burnham, *How Artificial Intelligence Is Transforming Logistics,* MIT MGMT. (Aug. 20, 2024), https://mitsloan.mit.edu/ideas-made-to-matter/how-artificial-intelligence-transforming-logistics.

[7] William J. Broad, *Google Introduces A.I. Agent That Aces 15-Day Weather Forecast,* N.Y. TIMES (Dec. 12, 2024), https://www.nytimes.com/2024/12/04/science/google-ai-weather-forecast.html.

*(A) the owner thereof has taken reasonable measures to keep such information secret; and*

*(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.*[8]

The Economic Espionage Act of 1996[9] provides federal criminal penalties for trade secret theft to "benefit any foreign government"[10] or "for use in interstate or foreign commerce, to the economic benefit of anyone other than the [trade secret] owner."[11] In 2016, Congress introduced a federal private right of action for trade secret misappropriation by enacting the Defend Trade Secrets Act (DTSA).[12]

The DTSA complements longstanding state frameworks for litigating civil trade secret cases.[13] For much of the 20th century (and to some extent today), trade secret common law was guided by the First Restatement of Torts, published in 1939 by the American Law Institute.[14] In the late 1960s, the Uniform Law Commission began work to develop the Uniform Trade Secrets Act (UTSA) model legislation.[15]

The UTSA, which "codifies the basic principles of common law trade secret protection,"[16] was published in 1979 and then revised in 1985,[17] and has since been enacted (with some variations)[18] in nearly all U.S. states and in the District of Columbia.[19]

---

[8] 18 U.S.C. § 1839(3).

[9] Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (1996).

[10] 18 U.S.C. § 1831(a).

[11] 18 U.S.C. § 1832(a).

[12] Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (2016).

[13] There are also criminal laws at the state level addressing trade secret theft. *See, e.g.*, CAL. PENAL CODE § 499c (Deering 2024) and TEX. PENAL CODE § 31.05 (West 2023).

[14] RESTATEMENT OF TORTS §757 cmt. b, (AM. L. INST. 1939).

[15] UNIF. TRADE SECRETS ACT WITH 1985 AMENDS. prefatory note at 1, 3 (UNIF. L. COMM'N 1985), https://wipolex-res.wipo.int/edocs/lexdocs/laws/en/us/us034en.pdf.

[16] *Id*. at 1.

[17] "On August 9, 1979, the Act was approved and recommended for enactment in all the states . . . On August 8, 1985, [] four clarifying amendments were approved and recommended for enactment in all the states." *Id*. at 3.

[18] For a state-by-state comparison of state trade secret laws to the UTSA as of the late 2010s, see *Trade Secrets Laws and the UTSA: 50 State and Federal Law Survey*, BECK REED RIDEN LLP (Jan. 24, 2017), https://beckreedriden.com/trade-secrets-laws-and-the-utsa-a-50-state-and-federal-law-survey-chart/.

[19] *See* UNIF. TRADE SECRETS ACT (UNIF. L. COMM'N 1979), https://www.uniformlaws.org/committees/community-home?CommunityKey=3a2538fb-e030-4e2d-

## "Open" AI Models Still Involve Trade Secrets

AI models are often described as "open" or "closed." While these terms imply a distinct binary categorization, the reality is more nuanced. In practice, openness lies along a spectrum.[20] For example, a company describing its model as "open" might release the weights resulting from the training process without releasing information about the data, source code, or methods that were used to obtain the weights.

Almost no for-profit companies will elect to release literally all of the information associated with their AI solutions, because to do so would directly undermine their business goals. In practice, "open" typically means "not fully closed." It means that a company has elected to release one or more categories of information about an AI solution, while withholding as confidential other (and presumably much more valuable) aspects of the solution. Thus, companies that release open AI models still have a strong interest in trade secret protections.

## Overly Broad AI Reporting Regulations Would Open the Door to Economic Espionage

There are well known approaches that companies can take to help protect their AI systems and data from economic espionage. But policymakers have a role as well. It is important to avoid promulgating new regulations that would result in the creation of federal or state government databases regarding U.S. AI assets that would put the integrity of those assets at risk. This concern is not merely theoretical.

For instance, an October 2023 Executive Order[21]—which has since been revoked[22]—would have required AI companies to report information about the "physical and cybersecurity measures taken to protect"[23] model weights associated with certain large AI models, as well as the location and computing power of "large-scale computing cluster[s]."[24] Such a database would immediately have become a prime target for state-sponsored hackers, and

---

a9e2-90373dc05792 (last visited Apr. 27, 2025) (indicating enactment in the District of Columbia and all U.S. states other than New York and North Carolina).

[20] *See, e.g.*, Andreas Liesenfeld & Mark Dingemanse, *Rethinking Open Source Generative AI: Open-Washing and the EU AI Act*, in FACCT '24: PROCEEDINGS OF THE 2024 ACM CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY (2024).

[21] Exec. Order No. 14,110, 88 Fed. Reg. 75,191 (Oct. 30, 2023).

[22] Exec. Order No. 14,179, 90 Fed. Reg. 8,741 (Jan. 23, 2025).

[23] Exec. Order No. 14,110, *supra* note 21, 75,197.

[24] *Id.*

if history is any guide,[25] those hackers would stand a strong chance of succeeding. With specific information about the cybersecurity measures used by AI companies in hand, the hackers would then be well positioned break into company systems and exfiltrate AI trade secrets.

## Overly Expansive AI Transparency Rules Would Undermine U.S. AI Leadership

AI regulatory proposals and statements of AI principles commonly address transparency. Calls for transparency reflect a natural desire to understand how an AI system works, particularly when it will be used in circumstances where system flaws may lead to harms. Balancing the equities involved in AI transparency requires considering both the broader societal interest in knowing what is occurring inside a company's AI "black box" and the company's right to maintain and protect the trade secrets it contains.

Overly expansive federal or state AI transparency requirements would force American companies to disclose trade secrets that are foundational to competitive differentiation, disfavoring American companies and undermining U.S. AI leadership. The concerns are particularly acute when mandated disclosure of detailed information about the inner workings of an AI system occurs pre-emptively, before there is any indication that an AI system has any flaws.

This does not mean that that transparency has no role in AI. But transparency requirements in any new AI regulations should be designed in a manner that allows companies to comply without putting their trade secrets at risk. When disclosure of AI trade secret information to the federal government is necessary for regulatory compliance, the government should provide an express assurance that it will retain the information as confidential.[26] Even with this assurance, compelled disclosure of AI trade secret information to the government should be strictly limited, because as discussed above, government databases risk being compromised.

---

[25] *See, e.g.*, Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES (July 9, 2015), https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html.

[26] This will ensure the information falls squarely within the scope of *Food Marketing Institute v. Argus Leader Media*, a 2019 Supreme Court decision concluding that "[a]t least where commercial or financial information is both customarily and actually treated as private by its owner and provided to the government under an assurance of privacy, the information is 'confidential . . . .'" 588 U.S. 427, 440 (2019).

## The Global Context Raises Additional Trade Secret Challenges

Many American AI companies operate globally, requiring them to comply with regulations in many different jurisdictions. The preeminence of American AI companies creates an asymmetry that has important consequences for regulation. Policymakers outside the U.S. may have less concern than their U.S. counterparts about the collateral damage to trade secrets resulting from rules requiring extensive levels of disclosure about the inner workings of an AI system.

The best approach to address U.S. AI company trade secrets in the context of the *global* regulatory environment is a topic for another day. I mention it here to underscore that as important as U.S. federal and state AI policies are, for the many U.S. AI companies that operate in dozens of non-U.S. jurisdictions, they are not the whole story.

## Corporate Trade Secret Overreach Can Impede Competition

Enabling U.S. AI companies to protect their trade secrets is vital to promoting a robust, competitive market for AI innovations. At the same time, overly broad assertions of trade secret scope have their own anti-competitive consequences. Nowhere is this issue more important than in relation to the ability of employees to change jobs.

The U.S. has extraordinary human capital in AI. In large and small companies, universities, government research labs, and beyond we have expertise in AI that is unique in the world. This ecosystem is so healthy in large part because it is dynamic—new companies are constantly being created, often by people who gain experience by working on AI at larger companies and then leave to found their own startups.

An engineer who has spent five years developing AI algorithms for an employer is not permitted to walk out the door with those algorithms. But the engineer is free to leave and then apply their general knowledge, skill, and experience regarding algorithm design to create brand new algorithms for a different company.[27] Just as it is vital for the U.S. legal system to allow companies to protect their AI trade secrets, it is also important to protect employees' rights to move between companies as long as they do so in a manner that respects the scope of legitimate claims on the trade secrets of their former employers.

In addition, AI trade secrets should not be used as a shield to sidestep liability. Examining the merits of a liability claim regarding an AI system will often require an inquiry into the detailed operation of the system, including through depositions of the system designers and examination of the source code by outside experts. Protective orders can be used to enable the defendant to disclose this information while still maintaining its trade secret status

[27] For a discussion of this aspect of trade secret law, see Camilla A. Hrdy, *The General Knowledge, Skill, and Experience Paradox*, 60 B.C. L. REV. 2409 (2019).

# AI Raises Novel Trade Secret Questions

AI can implicate trade secrets in many different ways. Trade secret law can protect an AI system's algorithm, source code, information in documents describing its design, the process of selecting and using training data, and knowledge gathered during testing regarding how to improve its performance. A company's plans for designing, building, and bringing an AI-based product or service to market can also qualify as trade secrets. Thus, in some ways, trade secret protection for AI is no different than for non-AI computer-based products and services.

However, there are novel trade secret law issues arising from the adaptive nature and complexity of AI systems, which creates a gap between the knowledge of the AI system designer and the actual behavior of the system. Because AI systems learn from their environment, they can operate in ways that can be elusive even to their designers. This creates a set of important questions at the intersection of AI with trade secret law, which developed under the assumption that a trade secret is known by its owner:

1) Can AI system designers hold trade secret rights regarding algorithms that they do not understand?
2) How does the lack of knowledge regarding an AI algorithm impact misappropriation claims?

I will address each of these questions in turn.

## Can AI system designers hold trade secret rights regarding algorithms that they do not understand?

I believe that the answer to this question is yes. To see why, consider what would happen if such rights were *not* provided.

Suppose that a company builds an AI system that, through adaptation, has evolved to the point where an algorithm it is executing is quite different from the one initially envisioned and programmed by its employees. After the adaptation process, the company employees no longer know *how* the algorithm works, but they do know *that it works extremely well* for its intended purpose. Assume further that the resulting algorithm is neither known nor readily ascertainable to others working in the same field of endeavor, and that it has economic value on that basis.

Now imagine that a rogue employee of the company instructs the AI system to output a human-readable description of the current algorithm. Before actually studying that description, the rogue employee leaves their employment to start a competing business. Thus, at the moment the rogue employee walks out the door, there is still no human who knows the details of the algorithm.

After setting up the competing company, the rogue (now former) employee studies the human-readable algorithm description, gains an understanding of how the system works, and develops a competing product based on the same algorithm. It would belie logic to conclude that the information is not a trade secret, and that the company that originally developed the algorithm would therefore be foreclosed from pursuing a misappropriation claim.

The idea that a company or person can own a trade secret that they do not understand is fully consistent with current trade secret law. Statutory definitions of trade secrets recite the *lack of knowledge* of *non-owners* of trade secrets but do not explicitly mention the *affirmative knowledge* of *owners*. As defined in federal law, a trade secret must "derive[] independent economic value, actual or potential, *from not being generally known* to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information."[28] The UTSA, which is the basis for most state trade secret statutes, contains nearly identical language.[29]

## How Does the Lack of Knowledge Impact Misappropriation Claims?

*Holding* trade secret rights is different from *asserting* them. In the context of pursuing misappropriation claims for an AI algorithm developed through automated adaptation, asserting trade secret rights will require describing the algorithm. It will not be sufficient for plaintiffs to state, in effect, "we're not sure how our AI algorithm works, but whatever it is doing, it is our trade secret, and the defendant has misappropriated it."

In cases where the allegation is misappropriation of an AI generated algorithm, as distinct from the code for implementing it, a complaint will need to go beyond only describing it using very broad terms, such as "an AI-based algorithm for stock trading." Rather, the complaint will need to provide enough detail to meet the applicable pleading standard[30]—which in a growing number of courts is "particularity"[31] or "specificity."[32]

---

[28] 18 U.S.C. § 1839.

[29] UTSA §1(4).

[30] Rule 8 of the Federal Rules of Civil Procedure, as interpreted by the Supreme Court in *Ashcroft v. Iqbal* (556 U.S. 662 (2009)), provides the general framework, but there is also trade secret-specific case law regarding pleading requirements.

[31] *See, e.g.*, Oakwood Labs. LLC v. Thanoo, 999 F.3d 892, 896 (3d. Cir. 2021) (quoting Diodes, Inc. v. Franzen, 260 Cal. App. 2d 244, 253 (1968)) (requiring "sufficient particularity" in a trade secret complaint).

[32] *See, e.g.*, Zirvi v. Flatley, 433 F. Supp. 3d 448, 465 (S.D.N.Y. 2020) (quoting ExpertConnect, L.L.C. v. Fowler, No. 18-cv-4828, 2019 U.S. Dist. LEXIS 114931, at *4 (S.D.N.Y. July 10, 2019)) ("[D]istrict courts

An AI algorithm trade secret misappropriation plaintiff will need to provide enough information in a complaint about the algorithm to survive a motion to dismiss. As the litigation progresses, the plaintiff will need to provide significantly more detail, so that the defendant (and the court) knows what specific information is at issue and can respond accordingly. A protective order can be used to ensure that the trade secret remains confidential during the litigation.

## Fear-Based Regulation Would Undermine U.S. AI Leadership

In the past several years there has been a steady drumbeat of calls to aggressively regulate AI. Sometimes, this is motivated by the premise—which I disagree with—that AI is an existential threat to humanity. Sometimes it is motivated by the view—which I also disagree with—that the best way for government to respond to AI is by subjecting it to an extensive new regulatory regime aimed at slowing AI down so that it can progress only as fast as policymakers allow.

If adopted in the U.S., this approach would directly undermine American AI leadership, as there are other countries—including geopolitical rivals—that will certainly avoid adopting policies centered on the goal of impeding AI development.

AI is a technology, and like any other technology, it can and will sometimes be misused. By analogy, the internet is also a technology, and it is undeniable that there are bad actors who use the internet to commit crimes. But if the federal government had imposed legislative and regulatory measures in the mid-1990s to intentionally slow down the growth and widespread adoption of the internet, the costs would have far outweighed the benefits.

It is also important to keep in mind that there is already a thicket of non-AI-specific law and regulation that will apply to AI. For example, if a bank uses an AI system to make home loan decisions in a manner that discriminates against a protected class, that is already actionable under the Fair Housing Act. A better approach is to limit new AI regulation to AI-driven harms that are not already addressed by existing non-AI-specific frameworks. To the extent such harms are identified, it does indeed make sense to examine what structures and incentives can be employed to mitigate them. But even then, any new regulation should be crafted in a manner that avoids collateral damage.

## AI Has Extraordinary Promise

AI promises to bring benefits to an almost endless list of applications, including pharmaceuticals, health care delivery, education, national defense, supply chain management, agriculture, weather forecasting, manufacturing, and financial services. For

---

in this circuit routinely require that plaintiffs plead their trade secrets with sufficient specificity to inform the defendants of what they are alleged to have misappropriated.").

America to be a global leader in realizing this potential requires a healthy AI innovation climate. That includes protecting AI trade secrets while also preventing their misuse to unfairly stifle competition. More broadly, it requires ensuring that AI entrepreneurs and investors continue to view the U.S. as the best country to start and grow the AI businesses of the future.

---

In closing, I would like to thank the Members of the House Judiciary Committee Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet for the opportunity to participate in today's hearing. I look forward to contributing to the dialog today and in the future on ways to ensure the continued prosperity of the American AI ecosystem.