

PROTECTING OUR EDGE: TRADE SECRETS AND THE GLOBAL AI ARMS RACE

HEARING

BEFORE THE

SUBCOMMITTEE ON COURTS, INTELLECTUAL
PROPERTY, ARTIFICIAL INTELLIGENCE, AND
THE INTERNET

OF THE

COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

WEDNESDAY, MAY 7, 2025

Serial No. 119-19

Printed for the use of the Committee on the Judiciary



Available via: <http://judiciary.house.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2025

COMMITTEE ON THE JUDICIARY

JIM JORDAN, Ohio, *Chair*

DARRELL ISSA, California	JAMIE RASKIN, Maryland, <i>Ranking Member</i>
ANDY BIGGS, Arizona	JERROLD NADLER, New York
TOM MCCLINTOCK, California	ZOE LOFGREN, California
THOMAS P. TIFFANY, Wisconsin	STEVE COHEN, Tennessee
THOMAS MASSIE, Kentucky	HENRY C. "HANK" JOHNSON, JR., Georgia
CHIP ROY, Texas	ERIC SWALWELL, California
SCOTT FITZGERALD, Wisconsin	TED LIEU, California
BEN CLINE, Virginia	PRAMILA JAYAPAL, Washington
LANCE GOODEN, Texas	J. LUIS CORREA, California
JEFFERSON VAN DREW, New Jersey	MARY GAY SCANLON, Pennsylvania
TROY E. NEHLS, Texas	JOE NEGUSE, Colorado
BARRY MOORE, Alabama	LUCY MCBATH, Georgia
KEVIN KILEY, California	DEBORAH K. ROSS, North Carolina
HARRIET M. HAGEMAN, Wyoming	BECCA BALINT, Vermont
LAUREL M. LEE, Florida	JESÚS G. "CHUY" GARCÍA, Illinois
WESLEY HUNT, Texas	SYDNEY KAMLAGER-DOVE, California
RUSSELL FRY, South Carolina	JARED MOSKOWITZ, Florida
GLENN GROTHMAN, Wisconsin	DANIEL S. GOLDMAN, New York
BRAD KNOTT, North Carolina	JASMINE CROCKETT, Texas
MARK HARRIS, North Carolina	
ROBERT F. ONDER, JR., Missouri	
DEREK SCHMIDT, Kansas	
BRANDON GILL, Texas	
MICHAEL BAUMGARTNER, Washington	

SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, ARTIFICIAL INTELLIGENCE, AND THE INTERNET

DARRELL ISSA, California, *Chair*

THOMAS MASSIE, Kentucky	HENRY C. "HANK" JOHNSON, JR., Georgia,
SCOTT FITZGERALD, Wisconsin	<i>Ranking Member</i>
BEN CLINE, Virginia	ZOE LOFGREN, California
LANCE GOODEN, Texas	TED LIEU, California
KEVIN KILEY, California	JOE NEGUSE, Colorado
LAUREL LEE, Florida	DEBORAH ROSS, North Carolina
RUSSELL FRY, South Carolina	ERIC SWALWELL, California
MICHAEL BAUMGARTNER, Washington	SYDNEY KAMLAGER-DOVE, California

CHRISTOPHER HIXON, *Majority Staff Director*

JULIE TAGEN, *Minority Staff Director*

C O N T E N T S

WEDNESDAY, MAY 7, 2025

OPENING STATEMENTS

	Page
The Honorable Darrell Issa, Chair of the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet from the State of California	1
The Honorable Henry C. “Hank” Johnson, Ranking Member of the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet from the State of Georgia	2
The Honorable Jamie Raskin, Ranking Member of the Committee on the Judiciary from the State of Maryland	3

WITNESSES

Benjamin Jensen, Ph.D., Director, Senior Fellow, Center for Strategic and International Studies Futures Lab	
Oral Testimony	6
Prepared Testimony	9
John Villasenor, Professor of Electrical Engineering, Law, Public Policy, and Management, University of California, Los Angeles	
Oral Testimony	18
Prepared Testimony	20
Christopher A. Mohr, President, Software and Information Industry Association	
Oral Testimony	31
Prepared Testimony	33
Helen Toner, Director of Strategy and Foundational Research Grants, Georgetown University Center for Security and Emerging Technology, Georgetown University	
Oral Testimony	47
Prepared Testimony	49
Nicholas Anderson, President, Chief Operating Officer, Invictus International Consulting, LLC	
Oral Testimony	57
Prepared Testimony	59

LETTERS, STATEMENTS, ETC. SUBMITTED FOR THE HEARING

All materials submitted for the record by the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet are listed below	82
A report entitled, “AI Talent Report,” Jan. 14, 2025, <i>Council of Economic Advisers (CEA), The White House</i> , submitted by the Honorable Sydney Kamlager-Dove, a Member of the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet from the State of California, for the record	

QUESTIONS AND RESPONSES FOR THE RECORD

Questions from the Honorable Darrell Issa, Chair of the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet from the State of California, for the record
Questions to Nicholas Anderson, President, Chief Operating Officer, Invictus International Consulting, LLC
Response to questions from Nicholas Anderson, President, Chief Operating Officer, Invictus International Consulting, LLC
Questions to Benjamin Jensen, Ph.D., Director, Senior Fellow, Center for Strategic and International Studies Futures Lab
Questions to Christopher A. Mohr, President, Software and Information Industry Association
Response to questions from Christopher A. Mohr, President, Software and Information Industry Association
Questions to John Villasenor, Professor of Electrical Engineering, Law, Public Policy, and Management, University of California, Los Angeles
Response to questions from John Villasenor, Professor of Electrical Engineering, Law, Public Policy, and Management, University of California, Los Angeles

PROTECTING OUR EDGE: TRADE SECRETS AND THE GLOBAL AI ARMS RACE

Wednesday, May 7, 2025

HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, AND
ARTIFICIAL INTELLIGENCE, AND THE INTERNET

COMMITTEE ON THE JUDICIARY

Washington, DC

The Committee met, pursuant to notice, at 10 a.m., in Room 2141, Rayburn House Office Building, the Hon. Darrell Issa [Chair of the Subcommittee] presiding.

Members present: Representatives Issa, Massie, Fitzgerald, Cline, Fry, Johnson, Ross, and Kamlager-Dove.

Mr. ISSA. The Subcommittee will come to order. Without objection, the Chair is authorized to declare a recess at any time.

We welcome today our guests for a hearing on Trade Secrets in the Global AI Arms Race. I now recognize myself for a short opening statement.

Today's hearing addresses the core tension in the age of artificial intelligence to push for disclosure, balanced with the need to protect innovation that drive U.S. leadership. There is a nondisclosure on the phone.

The proprietary algorithms that, in fact, train data sets are likely to be now and in the future the secret sauce, not patented, not available to the public, but of such value that other nefarious actors will do anything to get them. Without strong protections, we risk sacrificing the very breakthroughs we aim to encourage. Some have called the sweeping AI disclosure mandates in the name of transparency. This Committee has strongly believed and will continue to believe in transparency, but like anything else, a protective order is just a promise and a promise that is historically not kept, in fact, has no value.

We cannot require disclosure of trade secrets or proprietary data sets under the guise of transparency. Such disclosures would not only have a chilling effect on innovation, but hand strategic advantage to foreign adversaries who do not play by the same rules. Consider this. The United States' investment in AI is approaching \$1 trillion. China has invested not more than one third as much and is already neck to neck with the United States. The DeepSeek and other Chinese models are rapidly catching up to American compa-

nies. Let's look deeper. The DeepSeek contains models that clearly were taken from OpenAI and other sets. We know China's speed is not merely because they invest in innovation. It is also the result of IP theft, reverse engineering, and efforts to circumvent U.S. export controls and more.

China has also weaponized our legal system by financing lawsuits that target American firms in expensive litigation and with the intent, in many cases, to mine that proprietary information. All the while, China continues to refuse meaningful protections on U.S. IP in its own courts. I personally have been part of that recognition that they will not defend trademarks, patents, even when you go to the expense of getting them in China, even if you make your product in China, you will not be protected.

Last, American companies have a reverse situation, one in which we are working constantly, and this Committee has worked tirelessly on a bipartisan to promote rocket docket to, in fact, get the speed of decision to the lowest cost in the quickest time. Well, in China, you can be assured if you are an American company asserting your rights, you will go into the Never-Neverland of your case will come up some day.

Efforts continue to include the need to prevent U.S. engineers with access to specific sensitive AI systems from sidestepping non-competes and NDAs by working for Chinese firms. Ensure the disclosure regimes do not inadvertently reveal protection by mirroring EU-style regulations. I might say here, a little off the record, EU, as we speak, is second guessing their very disclosures. It has not escaped us that the AI Act of Europe, in fact, was a great step forward and as we speak many are pushing to take at least a small step backward. With that, I am delighted to introduce my Ranking Member for his opening statement.

Mr. JOHNSON. Thank you, Mr. Chair. One hundred and 17 days ago, the Chinese company DeepSeek launched its flagship model, DeepSeek-R1. In the following days and weeks, American experts wrung their hands and shook their heads, many considering for the first time the possibility that we may be losing the so-called AI arms race.

The DeepSeek claims R1 was developed faster and cheaper than comparable U.S. models. Others argue DeepSeek at a minimum violated OpenAI's terms of service to obtain proprietary training data. Where everyone seems to agree is that AI startups should be innovating faster. I have heard colleagues suggest we should forget regulations, ignore IP laws and just focus on clearing the way for AI companies. I agree everyone wins when we foster American AI startups, but I think it is a false choice to say we can succeed only if we do so irresponsibly.

If you walk around the Capitol today you can see plants sprouting out of the soil beginning to grow. What you will notice if you look closely is some of those shoots growing in the shade look like they are growing faster than the others. As they race for just a little bit of sunlight, yes, they grow quickly, but ultimately, they grow less hardy, more brittle, and prone to disease. AI innovation works the same way. As we seek ways to promote American AI startups, we should also work to ensure that businesses meet minimum standards for system cybersecurity. We should ask what types of

transparency are necessary to protect other IP rights and consider how to set standards while still protecting trade secrets. By encouraging companies to meet best practices and respect intellectual property rights, we will foster hardy competition that protects U.S. innovation from those who seek to undermine our success.

The Government of China has made no secret of its intent to steal American intellectual property and there is bipartisan agreement that the United States should protect its innovations from those who seek to benefit from American ingenuity. There is also a right way and a wrong way to compete with our adversaries. While we don't always agree on this Committee, we have had meaningful discussions on the right to protect American IP from the Government of China, cybersecurity standards to keep our people and our institutions safe, and the threat landscape to AI innovation.

The only trouble, on the other hand, has acted in ways that hurt American businesses. His ideologically inconsistent and unpredictable tariffs have hurt American consumers, American businesses, and our allies. Innovation in America suffers when the path forward is uncertain. For generations, American companies have benefited from attracting the best and the brightest from other Nations, yet, seemingly without reason, Trump again and again hurts American businesses by attempting to revoke already granted student visas and threatening the H1B visa program for highly skilled immigrants.

The deleterious impact of these policies on AI innovation should not be ignored. According to a recent study, immigrants founded or cofounded 28 of the top 43 AI companies in the United States and 70 percent of full-time graduate students in fields related to artificial intelligence are international students. Instead of focusing on policies that stand to derail American innovation, we should focus of upholding our treaties and respecting our allies. We should encourage our research institutions to engage with universities around the world. The breakneck speed of innovation has made it easier than ever to reach out to people around the world. Now, is not a time for isolationism because history has shown us that true innovation thrives on openness. After all, groundbreaking inventions rarely emerge when knowledge is walled off.

I thank the witnesses for being here today and I yield back.

Mr. ISSA. The gentleman yields back. We now recognize the Ranking Member of the Full Committee for his opening statement.

Mr. RASKIN. Thank you very much, Mr. Chair, and thanks to the witnesses for joining us. I am happy to participate in a rare hearing on the important bipartisan work of this Committee. We don't agree on a lot these days, but the importance of the U.S. intellectual property regime to American innovation is indeed a value that we all share. Even with this agreement in Congress, the Executive Branch has injected terrible instability into our intellectual property regime.

Innovation depends on stable and predictable rules the people can rely on to secure their inventions and property rights, manufacture their products, and attract investors and consumers to their businesses. Instead of fostering a stable atmosphere which allows people to innovate, the Trump Administration has hampered cre-

ativity. Since he was inaugurated, Trump has revoked Federal research grants to universities where scientists make significant new discoveries every year. He has tried to take over some universities. He has tried to cancel student visas. Last time he was President, of course, he increased the denial for highly skilled immigrants who work in engineering, computer programming and at research labs in highly technical fields.

Already in the first quarter of this year, Donald Trump's trade war against the world, except for Russia, has reduced the U.S. gross domestic product. It has raised prices for consumers and it has encouraged businesses to hoard goods. Chaotic tariffs that change from day to day make it difficult for businesses to plan ahead and result in them taking fewer risks. Companies are then less likely to invest in ideas and innovators are, in turn, less likely to strike out on their own.

We may never know what inventions, life-saving cures, world-changing businesses are being sacrificed at the altar of Donald Trump's helter skelter and lawless tariff agenda. We should also remember that investors and creators aren't just big businesses.

The heart of our IP system, our parents tinkering with an invention at the kitchen table after putting the kids to sleep, aspiring song writers, waiting tables to pay the bills while chasing their dreams, and engineering students researching the next big idea. Yet, now all these people are having a tough time in Trump's America, a place where hope of that next big break feels further and further away. Investing in ideas is a risky proposition, but it is even riskier for the individual who has to go it alone.

Finally, in most cases intellectual property ownership is only as good as the ability to enforce that right in court. Every rights holder should be worried as we watch the all-out assault on the Judicial Branch unfold. A judicial system that doesn't work for everyone eventually won't work for anyone and that includes IP owners. Despite these threats, the U.S. IP system is still lauded around the world for its ability to spur innovation and creativity. That is in part because our Founders chose to promote innovation by protecting the rights of individual creators. In the *Federalist 43*, Madison wrote that, "the utility of this power will scarcely be questioned," and in the case of patents and copyrights, the public good fully coincides with the claims of individuals. Rewarding individual discoveries and creations has allowed innovation to flourish.

According to a recent study, the U.S. is home to over half of the more than 10,000 AI startups across the 10 countries leading in AI. We should be proud of our AI leadership. We must also take steps to protect American trade secrets from competing nations that seek to steal our technology. Some have referred to the push to develop the most advanced AI model as the AI arms race. Now, there is nothing wrong with competition in this sense, but when other countries threaten U.S. cybersecurity, steal our inventions, and conduct economic espionage against U.S. companies as the Government of China has done, that is cause for serious scrutiny. Just because we all agree AI systems should be secure from foreign threats, does not obviate the responsibility, of course, that AI platforms have to other rights holders and to consumers.

Jack Dorsey and Elon Musk both recently made the claim that we should delete all IP law. I think that we can all emphatically reject that notion. America's intellectual property system has not just made us a global leader in AI; its very foundation created the careers of those two men. Intellectual property is the engine that powers our economy, drives innovation, jobs, and growth at every turn for all inventors, big and small, including Dorsey and Musk. Without a strong IP system, we risk losing the very spark that has made us such a leader in global innovation and opportunity.

I look forward to hearing from our witnesses today and I thank you, Mr. Chair, and yield back.

Mr. ISSA. Without objection, all other opening statements will be included in the record.

It is now my pleasure to introduce our panel of witnesses.

Mr. Nicholas Anderson. Mr. Anderson is President and Chief Operating Officer of Invictus International Consulting Company which provides technical services for national security systems. He previously served as Chief Information Officer for public sector at Lumen Technologies and served at the Department of Energy, Office of Management and Budget, and the Department of the Navy, Coast Guard, and served on active duty as a United States Marine which I presume means that he has been to Camp Pendleton in my District. It is a rite of passage.

Dr. Benjamin Jensen. Dr. Jensen is the Director of Future Labs and a Senior Fellow with the Defense and Security Department at the Center for Strategic and International Studies. He is also the Frank E. Petersen Chair for Emerging Technologies and a Professor of Strategic Studies at the Marine Corps University—I knew you were asked for a reason—on Advanced Warfare. Dr. Jensen previously served as Senior Research Director of the U.S. Cyber Solarium Commission and is a Reserve Officer in the United States Army. Double dipping.

Mr. Christopher Mohr. Mr. Mohr is President of the Software Information Industry Association, a collection of entertainment, consumer, and business software companies. He previously served as Senior Vice President for Intellectual Property and General Counsel at that organization and continues to serve as the Chief Legal Officer for the association.

Ms. Helen Toner. Ms. Toner is the Director of Strategies and Foundation Research Grants at Georgetown Center for Security and Emerging Technology. She previously served as Senior Research Analyst at Open Philanthropy where she advised policymakers and grantmakers on AI policy and strategy.

Dr. John Villasenor is Professor of Electrical Engineering, Law, Public Policy, and Management and the faculty Codirector at the Institute for Technology, Law, and Policy at UCLA. The professor works and his work is focused on technology and law-related to artificial intelligence, digital communication, computing, network, cybersecurity, and privacy.

We welcome our witnesses here today and pursuant to the Committee's rules, I would ask that you all rise to take the oath and the right hand is always good to use.

Do you solemnly swear or affirm under penalty of perjury that the testimony you will give will be true and correct to the best of your knowledge and information?

Please be seated. Let the record reflect that all witnesses answered in the affirmative.

Another part you have all seen on CSPAN, we would like you to stay as close as you can to five minutes. The lights on in front of you will count you down and indicate when you are close to, and then finally when you hit five minutes. Rest assured that not only will all your opening statements in their entirety be included in the record, but additional information that you provide or that later you provide pursuant to questions or things which are stimulated by our discussion. You really get hours and hours, you just get five minutes up front.

Dr. Jensen.

STATEMENT OF BENJAMIN JENSEN

Mr. JENSEN. Thank you, Chair, Ranking Member Johnson, and the Members of the Subcommittee. Before I start, I view my job here today to really help frame a larger conversation. That conversation really is about the defining competition of the 21st century and that is the race to shape what we are starting to call agentic AI. When I say agentic AI, I am not just talking about everybody playing with an LLM here or there or narrow imagery recognition. I am talking about the next level where all these applications start to work together and they start to generate actual knowledge, influence our decisions, and even help us manage complex tasks at scale. Frankly, whoever leads this agentic AI race is going to shape the rules of the future international order and I am not being hyperbolic. I sincerely mean that. If you talk about the efficiencies, the economic growth, the changing questions of governance, we are literally at the historical inflection point which made it so good to hear you bring in the *Federalist Papers* because we almost have to really think at that level about these tasks.

The stakes could not be clearer. This is not just about AI as a tool of human flourishing or who makes more money or who makes a better poem with an app. This is really about whether or not this is going to be a mechanism for authoritarian control or a way to really embody and propagate the best traditions and values on which our Republic was founded. I really mean it about the stakes. Frankly, while America has been the leader of this, the pioneer, and you can go back to the invention of the term artificial intelligence at Dartmouth, all the early engineering from Cornell to other universities, as you point out, this kind of basic research plus the beauty of capitalism working together. Frankly, that is under assault. The People's Republic of China is exploiting our economy and our innovation ecosystem. Beijing is basically conducting a coordinated strategy that siphons off intellectual property, circumvents export controls, and exploits legal gaps with State-directed theft and replication, Chair, what you have accurately characterized as weaponizing our legal system against us.

For at least today I want to talk about three ways the strategy unfolds, some technical, some more general. First, through knowledge distillation and what is called unbounded consumption at-

tacks, Chinese firms replicated U.S. foundation models, so think OpenAI's ChatGPT, at a fraction, a fraction of the cost, not talking \$1 billion to develop a model, we are talking millions of dollars. A significant economic difference. Essentially what they did is they harvested the outputs of American models, definitely without permission, and used them to build their own versions like DeepSeek. Bluntly, this is not innovative. This is intellectual looting.

Second, through State sponsored cyber espionage, Chinese APT, Advanced Persistent Threat, groups like Salt Typhoon and others target everything from our cloud infrastructure to semiconductors. Increasingly, this isn't just random smash-and-grab hacking. It is a calculated campaign to steal what free societies and free people create.

Third, despite export controls, China continues to access critical chips and software. Export controls have utterly been futile up to this point and really make us have to rethink what is our defensive play book and what is our offensive play book.

Through loopholes, third party countries and subsidies, they keep advancing while American firms face regulatory burdens and shrinking market access. In short, the current approach is not enough. Export controls and AI diffusion policy do more economic harm than good. As you pointed out, Representative Johnson, we really have to protect the smaller innovators. How are we going to balance that?

If the Chinese Communist Party and its network of little giants and firms with parties the State control are using this playbook of steal, copy, accelerate, what do we do? Well, first America is never powerless. We at the time that we act decisively and we preserve our AI leadership, and I think there are three things that we can discuss along those lines.

First, we modernize intellectual property laws, and that we have amazing experts to talk to you about that. We need to address techniques like knowledge distillation and API abuse. We need to basically coordinate globally so it is not just in U.S. courts, it is other free society courts where we can bring this to bear. We even start to imagine—I love that you brought up again *Federalist 43*, what would that look like written in 2025? What would that look like if a legal scholar, using an LLM wrote it as a basis for us to start this conversation about what are property laws?

Second, we may need to start treating AI companies like critical infrastructure. Their products support national security, economic competitiveness, and global influence and those designations mean that you can work across jurisdiction with other Subcommittees and other Committees to start to think about tax credits and other incentives that get you what you were talking about. How do you defend their IP?

I will close with saying we go on the offense. Lawsuits alone will not deter coordinated State-backed theft campaigns, so we have to prioritize the type of intelligence collection that can be declassified and turned into legally admissible information that can use to hold China accountable in multiple courts. Frankly, even consider the type of offensive cyber action that makes them think twice about stealing from America.

In closing, this is way more than about company profits. It is about free societies and nonauthoritarian regimes, assuming leadership of the coming AI century. I thank you for your time and I welcome your questions in the comment period.

[The prepared statement of Mr. Jensen follows:]



**Statement before the House of Representatives Committee
on the Judiciary Subcommittee on Courts, Intellectual
Property, and the Internet**

***“Protecting Our Edge: Trade Secrets and
the Global AI Arms Race”***

A Testimony by:

Benjamin Jensen, PhD

Director and Senior Fellow, CSIS Futures Lab

Frank E. Petersen Chair, School of Advanced Warfighting, Marine
Corps University

May 7, 2025

Rayburn House Office Building

Chairman Issa, Ranking Member Johnson, and distinguished Members of the Subcommittee, thank you for the opportunity to testify today on a matter of critical importance to the future economic prosperity and national security of the United States: maintaining American leadership in artificial intelligence (AI).

We are entering the era of agentic AI, in which algorithms will manage multiple complex processes in a manner that fundamentally change how we work, live, and govern.¹ Free societies led by the US made this new epoch possible.

While the US has been at the forefront of the theory and engineering that started in the 1950s and grew into the new world we confront today, its position is being challenged by the People's Republic of China (PRC). In short, the race to dominate the agentic era is now a central feature of 21st century great power competition. In this confrontation, failing to protect American innovators risks ceding the century to the Chinese Communist Party.

At the same time, with new technology comes new legal and economic questions. The strength of an open, free society is that the circulation of ideas helps its citizens imagine and build the future. Yet, authoritarian regimes like the CCP exploit this openness to steal a march illicitly acquiring U.S. intellectual property (IP), trade secrets, technological know-how, and sensitive data. As a result, the fundamental question before this committee is how to protect American innovation without sacrificing the very openness and creativity that makes it possible.

To address this challenge, I want to highlight three areas:

- 1) Disrupting Methods the PRC uses to Hijack U.S. AI models
- 2) Deterring Cyber Espionage in the Era of Agentic AI
- 3) The Futility of Export Restrictions

These challenges eclipse the tool kits currently used to protect American innovators and citizens. New methods, from laws to better aligning federal executive agencies, are needed to meet the challenge head on. Three standout:

- 1) Modernizing Intellectual Property Protections for the AI Era
- 2) Strengthen Cybersecurity and Treat AI Companies as Critical Infrastructure
- 3) Escalate to Active Defense and Offensive Operations Against Systemic IP Theft

Challenge 1: Disrupting Methods the PRC uses to Hijack U.S. AI models

¹ Mark Purdy "What is Agentic AI and How Will It Change Work?" *Harvard Business Review* December 12, 2024, online: <<<https://hbr.org/2024/12/what-is-agentic-ai-and-how-will-it-change-work>>>; Alex Wang on Why China Can't Be Allowed to Dominate AI-Based Warfare" *The Economist* March 4, 2025 <<<https://www.economist.com/by-invitation/2025/03/04/alex-wang-on-why-china-cant-be-allowed-to-dominate-ai-based-warfare>>>; Benjamin Jensen, Dan Tadross, and Matthew Strohmeyer "Agentic Warfare is Here. Will America Be the First Mover?" *War on the Rocks* April 23, 2025 <<<https://warontherocks.com/2025/04/agentic-warfare-is-here-will-america-be-the-first-mover/>>>.

An emerging threat to American AI leadership involves the replication of advanced AI models through methods such as "distillation". This technique allows a competitor to train a new, often smaller and more efficient, AI model (the "student") by feeding it vast amounts of output generated by a more powerful, pre-existing model (the "teacher"). Access to the teacher model's outputs is frequently obtained via its Application Programming Interface (API), potentially in violation of the provider's terms of service. The recent controversy involving U.S.-based OpenAI and the Chinese AI firm DeepSeek starkly illustrates this challenge. OpenAI has publicly accused DeepSeek of improperly using its API to exfiltrate large volumes of data. OpenAI alleges this data, generated by its proprietary models like ChatGPT, was then used via distillation to train DeepSeek's competing R1 reasoning model. Such actions would likely violate OpenAI's terms of service, which explicitly prohibit using API outputs to develop competing AI models. Supporting these allegations, Microsoft security researchers reportedly detected significant, anomalous data extraction patterns originating from OpenAI developer accounts believed to be affiliated with DeepSeek in late 2024. OpenAI subsequently blocked these accounts.

This case underscores the vulnerability of cutting-edge AI models to unauthorized replication through novel techniques that challenge existing legal frameworks. Current intellectual property laws, including copyright, patent, and trade secrets, were not designed to address the unique complexities of AI, such as the ownership of AI-generated outputs or the legality of model distillation. For instance, U.S. copyright law generally requires human authorship for protection, making it difficult to assert copyright over the outputs of an AI model used in distillation. Furthermore, distillation replicates the functionality and knowledge embedded in a model's outputs, rather than directly copying the underlying code or patented processes, making traditional infringement claims challenging beyond a breach of contract (Terms of Service). The alleged mechanism of API abuse also highlights that this is not merely an IP issue, but a significant cybersecurity challenge. It points to vulnerabilities in API security protocols, inadequate access controls, and insufficient monitoring for anomalous data exfiltration, potentially exposing AI firms to unbounded consumption attacks, in which manipulated input data allows an attacker to exceed data restrictions when using an AI model API.²

New technology creates new legal and regulatory quandaries that have significant economic implications. Take AI distillation. Is using a teacher model of a known market competitor to teach a student model illegal? DeepSeek used chatbots to bombard OpenAI's ChatGPT with questions and used the resulting answers to train its model and reduce the underlying computational costs associated with training its R1 as little as \$6 million.³ To put that in perspective, there are reports that ChatGPT 5 cost more than \$2 billion dollars to develop, 400 times the cost of ChatGPT 3 and 17 times the cost of ChatGPT 4. The cost to develop new

² Master Spring Ter "Consumption and How to Secure Your Spring Boot2.x APIs" *Medium* November 10, 2024 <<
<https://master-spring-ter.medium.com/owasp-api-security-top-4-unrestricted-resource-consumption-and-how-to-secure-your-spring-boot-3-x-42d2e506b39a>>>

³ Adiya Soni and Zaheer Kachwala „DeepSeek's Low-cost AI Spotlights Billions Spent by US Tech" *Reuters* January 29, 2025 <<
<https://www.reuters.com/technology/artificial-intelligence/big-tech-faces-heat-chinas-deepseek-sows-doubts-billion-dollar-spending-2025-01-27/>>>

models has tended to grow by 2.4 times per year, but likely will increase barring a new method as seen in the ballooning costs of ChatGPT 5.⁴

Yet, is distillation IP theft? There is a difference of opinion this committee must address. According to the White House and OpenAI, distillation is a new form of IP theft.⁵ According to a study by the US patent office there are divergent views of whether AI generated content can be copyrighted protected.⁶ When distillation takes advantage of techniques like unbounded consumption attacks, it almost certainly violates the terms of service.

Regardless in an agentic era the central question is whether AI output counts as “creative content.” Do lines of code have agency to produce original content? The legal community is split. AI models are trained with scrapped data - massive amounts of data that increases with each new version - which is why groups have sued copies like OpenAI claiming copyright infringement by multiple organizations including the *New York Times*.⁷

Challenge 2: Deterring Cyber Espionage in the Era of Agentic AI

Beyond legal questions about distillation techniques, there are major concerns about the depth of Chinese APT groups penetration into the modern IT infrastructure and cloud service providers alongside old fashion IP theft.⁸ China’s demonstrated track record of cyber espionage could further increase its ability to collect the mass amounts of data it needs to train new AI models even when firms seek to deny access.⁹ Take the case of SilkTyphoon.¹⁰ Since 2024, this group has used stolen API keys and other credentials to collect data of interest to the Chinese government. Accessing privileged data could allow Chinese researchers the ability to tailor generative AI models.

Here there is less legally gray area. Rampant cyber espionage, especially when it is linked to advancing narrow commercial interests, is illegal including under the Computer Fraud and Abuse Act (CFAA). The challenge is enforcement. How can the US make it more difficult to

⁴ Ben Cottier et al “How Much Does It Cost to Train Frontier AI Models?” *EpochAI* June 3, 2024

<<<https://epoch.ai/blog/how-much-does-it-cost-to-train-frontier-ai-models>>>

⁵ aura Italiano and Natalie Musucemi “OpenAI has Little Legal Recourse Against DeepSeek Tech Law Experts Say”

Yahoo News January 31, 2025 <<[⁶ United States Copyright Office. *Copyright and Artificial Intelligence Part 2: Copyrightability* January 2025](https://www.yahoo.com/news/openai-little-legal-recourse-against-150858401.html?guce_referrer=aHR0cHM6Ly93d3cud2luc3Rvbi5jb20v&guce_referrer_sig=AQAAAArXZc5imJWVNSHJ_92vh3Cvxivr89PZUWLeOhPKcDaW6uO1YPI_wGC-GADRHUUbZStcRS8RKIIABBgYth54UWMX5fqueIV86YSBPgOIMvkVpDYXMXJglo5xaszIM8M72u7uyk_P8VvEjrKZsUe4eRU5WaVN2ydtoZTtWJNnH3BZBo>></p>
</div>
<div data-bbox=)

<<<https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-2-Copyrightability-Report.pdf>>>

⁷ “Judge Allows Newspaper Copyright Lawsuit against OpenAI to Proceed” *AP* March 26, 2025

<<<https://apnews.com/article/nvt-openai-copyright-lawsuit-chatgpt-cc19ef2cf3f23343738e892b60d6d7a6>>>

⁸ Billy Perrigo “Every AI Datacenter is Vulnerable to Chinese Espionage” *Time* April 22, 2025 <<

<https://time.com/7279123/ai-datacenter-superintelligence-china-trump-report/>>>

⁹ Brandon Valeriano, Benjamin Jensen, Ryan Maness. *Cyber Strategy: the Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018).

¹⁰ Jai Vijayan “China’s Silk Typhoon APT Shifts to IT Supply Chain Attacks” *Darkreading* March 5, 2025

<<<https://www.darkreading.com/remote-workforce/china-silk-typhoon-it-supply-chain-attacks>>

steal US data? To date, and despite monumental past efforts by Congress to include the U.S. Cyberspace Solarium Commission, America has yet to find the right suite of mechanisms to deter mass cyber espionage.¹¹

Second, the semiconductor industry provides the essential hardware foundation upon which the entire AI ecosystem is built. Consequently, intellectual property related to semiconductor design and manufacturing is a prime target for theft, particularly by nations seeking to rapidly advance their domestic capabilities. The case involving ASML, the world-leading Dutch producer of photolithography equipment crucial for advanced chipmaking, and entities linked to China, illustrates this threat vividly. ASML sued Xtal Inc., a Silicon Valley startup founded by former ASML engineer Zongchang Yu, for stealing trade secrets and won over \$800 million.¹² Sadly, the settlement came after individuals linked to XTAL had already stolen over 2 million lines of code.¹³ The stolen IP was directly linked to DJEL, who the Chinese government gave approval to under a program known as “little giants.”¹⁴ As a result, ASML – a maker of advanced extreme ultraviolet lithography systems key to cutting-edge chips – asked customers not to do business with DJEL.

This case reveals several critical vulnerabilities. First, it highlights the targeting of extremely specialized and foundational technology – computational lithography optimization software – the compromise of which can have cascading effects throughout the technology ecosystem by enabling the production of more advanced semiconductors essential for AI. Second, the alleged use of parallel corporate entities in different jurisdictions (Xtal in the US, DJEL in China) points to a sophisticated method for circumventing legal accountability and facilitating cross-border IP transfer. Third, the apparent state endorsement of DJEL through “little giant” status and investment *after* its affiliate was found liable for massive IP theft severely undermines the deterrent effect of civil litigation and monetary damages alone. It suggests that such activities might be viewed as contributing to national technological goals, thereby insulating perpetrators from consequences within their home jurisdiction. Fourth, ASML’s reported difficulties in investigating DJEL directly in China and its recourse to warning customers underscore the practical challenges of international IP enforcement, particularly against entities potentially shielded by foreign governments, necessitating stronger government-to-government mechanisms.

Last, there is growing evidence that state-linked entities in China are trying to exploit AI foundation models associated with U.S. firms for malicious purposes. Google has published

¹¹ Montgomery, M., B. Jensen, E. D. Borghard, J. Costello, V. Cornfeld, C. Simpson, and B. Valeriano. 2020. Cyberspace Solarium Commission Report. Washington, DC. <https://www.solarium.gov/report>; Brandon Valeriano and Benjamin Jensen “Building a National Cyber Strategy: The Process and Implications of the Cyberspace Solarium Commission Report” *IEEE 13th International Conference*, 2021

<<<https://ieeexplore.ieee.org/document/9467806>>>
¹² “ASML Says Ex-Employees in China Stole Chip Data” Bloomberg February 15, 2023 <<[ASML Says Ex-Employee in China Stole Chip Data - Bloomberg](#)>>

¹³ “Engineer Who Fled Charges of Stealing Chip Technology in US Now Thrives in China” CSET June 6, 2022 <[Engineer Who Fled Charges of Stealing Chip Technology in US Now Thrives in China | Center for Security and Emerging Technology](#)>>

¹⁴ “ASML Warns Chinese Rival May Be Infringing Its Trade Secrets” Data Center Knowledge February 10, 2022 <<[ASML Warns Chinese Rival May Be Infringing Its Trade Secrets](#)>>

evidence of state-based actors in China seeking to exploit its Gemini model to refine propaganda as well as enhance its cyber capabilities, including using generative AI to obtain deeper access to target networks through privilege escalation, data exfiltration, and detection evasion.¹⁵

Challenge 3: The Futility of Export Restrictions

Recent reports have demonstrated the futility of existing export controls to limit AI advances in China.¹⁶ Despite U.S. restrictions, China has continued to access high-end export controlled chips.¹⁷ These shadow market includes using third-party firms.¹⁸ When combined with domestic investments as part of the PRC's civil-military fusion policy, this illicit activity ensures that the CCP has access to the computational power and IP required to build new generative AI models like DeepSeek.¹⁹

While export controls remain an important tool to slow adversary access to sensitive technologies, they have proven increasingly ineffective in the AI competition with China. The Biden administration's AI Diffusion Policy, introduced in 2025 to regulate the global spread of advanced AI systems, exemplifies both the necessity and the limits of this approach.²⁰ By categorizing countries into tiers, the policy aims to prevent adversaries like China from acquiring advanced chips, model weights, and critical software. Yet Beijing's playbook is not reliant on fair-market purchases alone. Chinese firms routinely evade restrictions through intermediaries, global subsidiaries, and gray market channels. They optimize AI workloads on restricted chips, leverage vast pools of open-source AI research, and accelerate indigenous semiconductor development subsidized by the state. These realities mean that while the AI Diffusion Policy may impose temporary friction, it does little to fundamentally constrain China's long-term trajectory. In a race defined by rapid innovation cycles and aggressive state backing, speed bumps are not barriers. For this reason, President Trump is right to explore significant changes to the policy.²¹

Moreover, policies like AI Diffusion risk harming U.S. technology leadership more than degrading China's ambitions. Export restrictions deny American companies access to lucrative

¹⁵ Google Threat Intelligence Group. Adversarial Misuse of Generative AI. January 29, 2025 <<
<https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai>>>

¹⁶ Ritwik Gupta, Leah Walker, and Andrew Reddie. "Whack-a-Chip: The Futility of Hardware-Centric Export Controls" arXiv 2411. <<<https://arxiv.org/pdf/2411.14425>>>

¹⁷ Josh Ye, David Kirton, and Chen Li. "Inside China's Underground Market for High-end NVIDIA AI Chips" Reuters June 20, 2023 <<<https://www.reuters.com/technology/inside-chinas-underground-market-high-end-nvidia-ai-chips-2023-06-19/>>>

¹⁸ Jack Burnham. "Seeking Decisive Edge, China Uses Third-Party Countries to Circumvent U.S. AI Export Controls" *Foundation for Defense of Democracy*, March 4, 2025 <<
https://www.fdd.org/analysis/policy_briefs/2025/03/04/seeking-decisive-edge-china-uses-third-party-countries-to-circumvent-u-s-ai-export-controls>>

¹⁹ Kenneth Ong. "China's Defiant Chip Strategy" FPRI June 28, 2024 <<
<https://www.fpri.org/article/2024/06/chinas-defiant-chip-strategy/>>>

²⁰ Matt Bracken. "Biden Administration Unveils Export Controls on AI Models, Chips" *Fedscoop* January 13, 2025 <<
<https://fedscoop.com/commerce-ai-diffusion-rule-biden-admin-industry-security/>>>

²¹ Karen Freifeld. "Trump officials eye changes to Biden's AI chip export rule, sources say" *Reuters* April 29, 2025 <<
<https://www.reuters.com/world/china/trump-officials-eye-changes-bidens-ai-chip-export-rule-sources-say-2025-04-29/>>>

markets, particularly in fast-growing AI sectors, while foreign competitors — less burdened by restrictions — fill the vacuum. Revenue losses erode the resources U.S. firms reinvest into frontier R&D, weakening long-term global competitiveness. Leading voices in the AI hardware ecosystem, such as NVIDIA, have strongly criticized the Biden Administration’s AI Diffusion rule as regulatory overreach that risks derailing innovation and ceding U.S. technological advantage. As NVIDIA argued, for decades, America’s strength has come from fostering open and competitive computing and software ecosystems — not dictating design, sales, and global market access.²² The company warns that the new rule, drafted with minimal transparency, seeks to impose sweeping government control over how semiconductors, computers, and software are marketed worldwide — restricting even mainstream technologies widely used in gaming PCs and consumer devices. Cloaked in national security language, such restrictions, they argue, will do little to stop China while directly undercutting U.S. global competitiveness and stifling the innovation that fuels economic growth and American influence.

Simply put, defensive measures like AI Diffusion, when deployed in isolation, can backfire: they limit U.S. firms, strain alliances, and slow innovation without stopping China’s systemic theft and replication efforts. To be effective, export controls must be paired with offensive measures — targeting theft, disrupting circumvention, and degrading stolen IP. Without this shift, current policies risk becoming self-imposed constraints while Beijing accelerates unchecked.

Taken together these challenges suggest three broad categories of action Congress can help set in motion to ensure the US retains the commanding heights in the coming agentic era.

1. Modernize Intellectual Property Protections for the AI Era

The first priority must be addressing the legal and regulatory blind spots surrounding intellectual property in an agentic economy. As this subcommittee’s important prior work on digital copyright and platform regulation has shown, emerging technologies often challenge legacy legal frameworks. Techniques like model distillation and unbounded consumption attacks—where API outputs are systematically harvested to train rival AI models—undermine the fundamental economics of AI innovation. These attacks are not only breaches of contract but strike at the intellectual core of American firms investing billions in foundation models. Congress should expand existing IP protections to clarify the legal status of AI-generated outputs, develop new statutory tools to criminalize intentional distillation that violates terms of service, and empower firms to take action against bad actors. Further, to avoid driving these activities offshore, the subcommittee should coordinate with counterparts in Commerce and Foreign Affairs to pursue international agreements that criminalize unauthorized model replication, creating unified global standards against this growing threat.

²² Ned Finkle “NVIDIA Statement on the Biden Administration’s Misguided AI Diffusion Rule” *NVIDIA* January 13, 2025 << <https://blogs.nvidia.com/blog/ai-policy/>>>

2. Strengthen Cybersecurity and Treat AI Companies as Critical Infrastructure

Second, cybersecurity must become a central pillar in defending U.S. AI leadership. While distillation attacks exploit legal gaps, Chinese espionage campaigns exploit technical vulnerabilities, including stolen API keys, cloud service intrusions, and access to development pipelines. This is not simply a civil issue — it is a national security threat. Congress should consider tax credits and other market-based incentives to encourage AI firms to increase their cyber defenses, invest in anomaly detection, and enhance user verification systems. The subcommittee should also work with counterparts on Homeland Security to ensure that AI firms are formally recognized as part of U.S. critical infrastructure under CISA’s framework. Doing so would unlock a broader range of federal support, including enhanced threat intelligence sharing, voluntary cybersecurity performance goals, and rapid incident response assistance. Given the evidence of state-backed actors targeting these firms to advance Chinese industrial policy, AI companies must be treated not just as technology providers, but as pillars of national resilience.

3. Escalate to Active Defense and Offensive Operations Against Systemic IP Theft

Finally, the United States must move from passive protection to active disruption. Defensive tools alone will not deter a nation like China, which uses a coordinated state-backed strategy combining espionage, legal loopholes, and market coercion. As a first step, Congress should ensure that the Intelligence Community and law enforcement prioritize collection on PRC IP theft campaigns, with a mandate to declassify evidence where possible. Providing DOJ and allied nations’ legal authorities with clear, court-admissible intelligence on state-directed theft will allow for more aggressive prosecution strategies and multilateral lawfare efforts. Diplomacy and technical standards-setting must also become offensive tools — rallying allies to adopt higher standards, coordinate enforcement, and close legal loopholes that allow Chinese firms to exploit jurisdictional arbitrage. In the most extreme cases, covert action should not be off the table. Just as the U.S. used software sabotage and misinformation programs in the 1980s to slow Soviet industrial espionage, tailored offensive cyber operations, data poisoning, and supply chain disruption efforts should be considered to degrade and delay the use of stolen U.S. intellectual property. In short, America cannot win this contest through defense alone. Restoring deterrence requires imposing real costs on state-backed IP thieves and making the economic and political risks of this strategy unbearable for Beijing and its proxies.

Why We Must Win the Agentic AI Race

At its core, this is not just a debate about intellectual property or cybersecurity. It is about strategic competition — and whether free societies will define the AI century or cede it to authoritarian regimes that view knowledge as power and power as control.

AI is no longer just a tool. We are entering the era of agentic AI — systems capable of generating new knowledge, accelerating scientific discovery, and shaping human decision-making at scale. Whoever leads in this domain will write the rules of the emerging international order. Beijing understands this. That is why China is not merely stealing technology opportunistically — it is waging a systematic campaign to siphon intellectual property, circumvent export controls, and exploit legal and technical gaps to build competitive AI ecosystems.

If China wins this race, AI will not become a catalyst for human flourishing. It will become a mechanism for surveillance, coercion, and influence. But if the United States and its allies prevail — if we defend IP, secure our digital frontiers, and go on offense against theft — AI can unlock new frontiers of growth, creativity, and global problem-solving. Free societies will innovate faster and more responsibly. Markets will remain open. Science will advance unshackled by censorship or central control.

That is why the stakes could not be higher. This is about more than defending the bottom line of U.S. firms — it is about defending a model of governance built on liberty and openness. History will not remember the lawsuits or regulations that defined the margins of this fight. It will remember whether we acted boldly enough to keep the commanding heights of the AI revolution in the hands of those who believe knowledge should empower, not oppress.

We cannot afford to lose the AI century to regimes that see agentic AI as the ultimate instrument of authoritarian control. The time to act — and to compete — is now.

Mr. ISSA. Thank you. Dr. Villaseñor.

STATEMENT OF JOHN VILLASEÑOR

Mr. VILLASEÑOR. Chair Issa, Ranking Member Johnson—

Mr. ISSA. Now, the little button in front when it turns red, it is a good sign.

Mr. VILLASEÑOR. Chair Issa, Ranking Member Johnson, Ranking Member Raskin, and the Members of the Subcommittee, thank you very much for the opportunity to testify here today. I should mention at the outset that I am testifying in my own individual capacity, and I am not representing any organization.

America is the clear global leader in AI, a technology that is foundational to our continued economic prosperity and national security. 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 innovated and market leading, they are ripe targets for trade secret theft.

Second, policy discussions regarding AI regulation here in the United States often give insufficient consideration to the potential collateral damage to trade secret threats. Given the enormous attention to generative AI products such as ChatGPT, it is important to keep in mind that AI is much more than generative AI. The recent advances in other areas of AI are equally impressive. For instance, AI is revolutionizing drug discovery. AI is also at the core of algorithms that enable autonomous vehicles to navigate complex city streets. Collaborations between humans and AI are promising to bring improvements to medical image interpretation. AI can extend the human capacity to create new inventions and will revolutionize logistics, weather forecasting and many other fields. AI is critical to ensuring strong national defense.

Overly expansive transparency rules would undermine AI leadership. Exhibit A for that would be, for example, the now-revoked Executive Order issued in October 2023, which would have required some AI companies to file with the Government information about the physical and cybersecurity measures used to protect their model weights. Clearly, if the Government were to maintain databases like that, those databases would become essentially a target list for cyber espionage, armed with the information hacked from those databases and those databases would get hacked, then State-sponsored actors could more easily enter the systems of leading AI companies.

There are novel trade secret issues arising from the adaptive nature and complexity of AI systems. Because AI systems learn from their environment, they can operate in ways that can be elusive even to their designers. This creates some really important and interesting questions.

First, can CRADAs of AI systems have trade secret rights in algorithms they do not understand? I believe that the answer to this question is yes. 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.

Does this algorithm qualify as a trade secret owned by the company, even though no human knows what it is? In my view it does.

Second, how can plaintiffs assert misappropriation of trade secrets they don't know? Well, the answer that asserting trade secret rights in an algorithm will require describing it which requires plaintiffs to learn it. It will not be sufficient for plaintiffs to State in effect we are not sure how our AI works, but whatever it is doing, it is our trade secret and the defendant has misappropriated it. Rather, plaintiffs will need to provide enough detail for a court and a defendant to know which specific trade secret is at issue.

I would also like to briefly mention the global context. The pre-eminence of American AI companies creates an asymmetry. Policy makers outside the U.S. may have less concern than their U.S. counterparts about the collateral damage to trade secrets resulting from AI regulations. They will have little incentive to regulate in a manner that preserves the competitive advantage of U.S. AI companies.

Finally, I would like to briefly comment on AI regulation more generally. 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 that the best way for Government to respond to AI is by subjecting it to an extensive new regulatory regime and that 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 countries, including geopolitical rivals, that will certainly avoid adopting policies centered on the goal of impeding AI development.

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, the use of a discriminatory AI system to make home loan decisions would already be unlawful under the Fair Housing Act.

In closing, I would like to thank the Members of the Subcommittee for the opportunity to participate in today's hearing and I look forward to your questions.

[The prepared statement of Mr. Villaseñor follows:]

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 1996⁹ 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://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 Order²¹—which has since been revoked²²—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 be 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 standard³⁰—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.

Mr. ISSA. Thank you. Mr. Mohr.

STATEMENT OF CHRISTOPHER A. MOHR

Mr. MOHR. Mr. Chair, Ranking Member Johnson, Ranking Member Raskin, and the Members of the Committee, on behalf of SIIA and its members, thank you for this opportunity to share our views.

The SIIA represents over 350 companies in the business of information. Our members range from startups to some of the largest and most recognizable corporations in the world. For over 40 years, we have advocated for the health of the information life cycle, advancing favorable conditions for its creation, dissemination, and productive use. Our members create educational software, search engines, e-commerce platforms, legal research and financial databases, and a variety of other products that people depend on in their day-to-day lives. We are the place where information and technology meet and occasionally collide.

The SIIA was founded on the premise of respect for intellectual property rights, especially around software. For decades, we helped our members enforce their copyrights against infringers, something we still do. Today, our members are building AI into many of their products and services. They actively use it in their media operations, in the classroom, in fraud detection, in market data, money laundering investigations, and in locating missing children. They have invested billions in its development, acquisition, and use. They also have intellectual property rights undergirding that investment including patent, copyright, and trade secret rights.

As both software and information become increasingly sold as services, the threat from IP theft has evolved. The most valuable part of technology may not be in simply copying and using it, although that is certainly a threat, but in figuring out how it works. Our members welcome competition within the bounds of legal rules. The problem is that not everybody follows them.

From the very first days of the adoption of the TRIPS Agreement in 1994, our members have had problems with State sanctioned IP theft by the PRC. Now, the PRC has stated that it wishes to leave the world in AI by 2030 and reduce reliance on foreign technology. It intends to leverage the communist system and achieve that leadership in key areas including smart devices and speech recognition, image and video recognition, and financial services to name just a few. Unfortunately, for us and to mix metaphors a bit, the dragon has not changed its stripes. It is actively involved in the theft of trade secrets in several ways, from the use of insider threats to cyber-attacks to forced technology transfer to investment in U.S. startups, the conditioning market access under divulging and proprietary information.

Legal rights are not the problem. Congress has adopted substantive rights governing trade secrets in the United States and a global framework to respect those rights. What is lacking is it means to sufficiently incentivize the Chinese Government to abide by those protections or to provide means to enforce those protections. While there is no perfect solution, Congress has tools that it can and should develop to further protect American AI develop-

ment from foreign theft and possibly sabotage. We would suggest four areas for congressional attention.

The first is cybersecurity, building and updating infrastructure to keep up with emerging and evolving threats is a constant project. Large companies have cutting-edge systems that they can use to protect their products and users. Smaller businesses lack such resources. The Government should continue to explore ways to help them.

Second, Congress should ensure that the Committee for Foreign Investment, or CFIUS, continues to serve as an effective way to address trade secret risk by making sure that its scope of review remains adequate to address those risks.

Third, Congress should assist the administration in working with our allies and partners to build AI infrastructure on trusted providers, adoption of Huawei and other PRC-located providers creates an unreasonable potential for trade secret theft.

Finally, while the legal framework for protecting trade secrets is well developed, an emerging area of concern involves the exploitation of the U.S. legal system to gain unauthorized access to trade secret information through third party litigation funding of patent disputes by sovereign wealth entities. The landscape around AI and intellectual property is constantly evolving and as technology continues to advance, new threats will emerge. That pattern is unlikely to stop any time soon and we commend the Subcommittee for continuing to monitor these issues and engage industry.

Thank you for your consideration of our views and I am happy to answer any questions.

[The prepared statement of Mr. Mohr follows:]



**Written Testimony of Christopher A. Mohr, President, Software & Information
Industry Association**

"Protecting Our Edge: Trade Secrets and the Global AI Arms Race"

**Before the Subcommittee on Courts, Intellectual Property, Artificial Intelligence,
and the Internet of the Committee on the Judiciary of the U.S. House of
Representatives**

May 7, 2025

I. Introduction

Mr. Chairman, Ranking Member Johnson, and members of the Committee, on behalf of the Software and Information Industry Association (SIIA) and its members, thank you for this opportunity to share our views on "Trade Secrets: Protecting our Edge on AI and the Global AI Arms Race."

SIIA represents over 350 companies in the business of information. Our members range from start-up firms to some of the largest and most recognizable corporations in the world. For over forty years, we have advocated for the health of the information lifecycle, advancing favorable conditions for its creation, dissemination, and productive use. Our members create educational software, e-commerce platforms, legal research and financial databases, and a variety of other products that people depend on in wide swaths of commercial life. We are the place where information and technology meet.

SIIA was founded on the premise of respect for intellectual property rights, especially around software. For decades, we helped our members enforce their copyrights against infringers – something we still continue to do. Much of the software business has changed: floppy disks turned into CDs, which turned into services, and now AI is being built into many, many member products and services.

Our members have wholeheartedly embraced the promise of AI and predict advances that will revolutionize information management, creation, analysis, and dissemination. They actively use AI on many fronts—in their media operations, in the classroom, in fraud detection, in market data, in money laundering investigations,

and in locating missing children. They have invested billions in its development, acquisition, and use. They also have intellectual property rights undergirding that investment, including patent, copyright, and trade secret rights.

It is in the intellectual property space that the United States has really led the world by leading the creation of a rules-based order—most notably through the Trade-Related Aspects of Intellectual Property Rights portion of the Uruguay Round, otherwise known as TRIPs.¹ Those rules have helped stimulate the innovation, growth, and global leadership of the U.S. information technology sectors, increasing productivity and creating millions of jobs domestically.

Not everyone follows these rules. Software and content piracy remain problems in developing markets. And as both software and information became increasingly sold as a service, the threat from IP theft changed: the most valuable part of technology may not be in simply copying and using it—although that is certainly a threat—but in figuring out *how* it works.

As this Committee knows, the software industries (in fact most if not all of the content industries) had problems with Chinese piracy since the earliest days of its accession to the WTO.² As the United States Trade Representative 301 Reports document, acquisition of intellectual property—often by illicit means—has been a consistent pattern that has spanned administrations.³ While piracy remains a problem, trade secret theft will far surpass it in seriousness if left unaddressed.

The People's Republic of China (PRC) is engaged in an ongoing, coordinated campaign to steal American intellectual property. This strategy is foundational to Chinese Communist Party (CCP) economic policy, allowing the PRC to produce knockoffs of American IP without the up-front costs in research and development. This strategy includes artificial intelligence (AI) and machine learning, both as a target of IP theft and as a tool to expand their cybercrime and intelligence efforts.

¹ [Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C](#), 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994) (hereinafter, "TRIPs").

² See generally Panel Report, [China - Measures Affecting the Protection and Enforcement of Intellectual Property Rights](#), WTO Doc. WT/DS362/R (adopted Mar. 20, 2009). See also United States-[Certain Measures Concerning the Protection of Intellectual Property Rights](#), WTO Doc. WT/DS542.

³ See, e.g., Office of the U.S. Trade Representative (USTR), [2025 Special 301 Report](#), at 23–25, 44–55 (Apr. 29, 2025), [2020 Special 301 Report](#), at 18–19, 39–47 (Apr. 1, 2020), [2015 Special 301 Report](#), at 20–21, 32–43 (Apr. 13, 2015), [2010 Special 301 Report](#), at 19–23 (Apr. 30, 2010).

Indeed, the PRC has made acquiring key technologies a national priority, and its aggressiveness has increased. In 2015, its Made in China 2025⁴ policy set forth several initiatives by which it intended to advance its manufacturing priorities. These include, for example:

- **Mandated Technology Transfer in Joint Ventures.** American firms looking to enter the Chinese market in certain technology sectors are required to partner with Chinese firms. Trade secret theft can occur when the U.S. company is required to disclose proprietary information, which happens all too often through either formal or informal requirements.
- **Acquisition of Foreign Technology.** The initiative encourages Chinese companies, including state-owned enterprises and state-backed funds, to invest in or acquire foreign high-tech firms. These targeted investments are designed to obtain advanced technologies and intellectual property, which are then adapted and integrated into the PRC's domestic industries. This "buying-in" of technology is a deliberate effort to close the innovation gap with Western competitors.
- **Government Policy Leverage.** The PRC uses a mix of tax incentives, regulatory standards, procurement policies, and licensing requirements to pressure foreign firms to localize production, shift R&D to the PRC, and transfer technology to domestic entities. These policies are often coupled with conditioned market access as leverage.⁵

The PRC has also adopted a similar strategy with respect to AI, stating that it wishes to lead the world in AI by 2030 and reduce reliance on foreign technology.⁶ It intends to leverage the communist system and achieve that leadership in key areas including smart devices and speech recognition, image and video recognition, and financial services (especially around fraud detection). It also supports open source sharing of AI development.

There is nothing inherently wrong with another nation seeking to improve its technological and industrial development or to use AI or open source. SIIA has long

⁴ People's Republic of China State Council, [Made in China 2025 \(English translation\)](#) (May 8, 2015).

⁵ See USTR, [Four-year Review of Actions Taken in the Section 301 Investigation: China's Acts, Policies and Practices Related to Technology](#) at 2 (2024); U.S. China Economic and Security Review Commission, [How Chinese Companies Facilitate Technology Transfer from the United States](#), at 2 (2019).

⁶ People's Republic of China State Council, [The New Generation AI Development Plan](#) (Jul. 20, 2017).

supported both open and closed source software development, and its members have developed and used open source models.

But we support that development within the confines of a rules-based regime: intellectual property laws as passed in the United States and exported through international agreement. If a firm decides that it wishes to keep its AI development information proprietary, that choice must be respected. And when it comes to AI, that proprietary value may come from many places: proprietary algorithms, neural network architectures, training data, data-harvesting processes, and the unique methodologies employed to train and fine-tune models. Notwithstanding the Phase I trade agreement signed in January of 2020 where China pledged to address U.S. concerns,⁷ trade secret theft remains a special problem around AI. AI may be the technology of the moment, but China is running the same playbook.

The balance of our testimony is designed to describe those intellectual property rules and how China is evading them. First, we describe the legal regime governing trade secrets. Second, we discuss our members' concern about China state-sponsored activities that violate this regime. And finally, we close with suggestions about things that Congress might do to address them.

II. Trade Secrets are a Recognized and Valuable Form of Intellectual Property

Trade secrets constitute a distinct category of domestically and internationally recognized intellectual property, safeguarding confidential business information that confers a competitive advantage upon its holder. Unlike patents or copyright, which have disclosure elements that advance innovation, trade secrets are rooted in theories of unfair competition that recognize the value of secret business operations and know-how that provide companies with legitimate market advantages and are appropriately shielded from competitors.

A. The Scope of Trade Secret Protection under U.S. Law

The scope of protectable trade secret information is deliberately broad, encompassing formulas, patterns, compilations, programs, devices, methods, techniques, or processes. A commonly cited illustration is the formula for Coca-Cola, long guarded as a valuable company asset. Other examples include curated customer lists, proprietary software source code, unique manufacturing techniques, and, increasingly relevant, the complex algorithms, model weights, and curated

⁷ [*Economic and Trade Agreement Between the Government of the United States of America and the Government of the People's Republic of China*](#) (Jan. 15, 2020).

datasets underpinning AI systems. Many of these items are not eligible for patent protection as abstract ideas.

The legal definition, widely adopted across the United States through the Uniform Trade Secrets Act (UTSA), establishes two core requirements.⁸ First, the information must derive independent economic value, actual or potential, from its secrecy; it cannot be generally known to the public or accessible to competitors through proper means.⁹ Second, the information must be the subject of efforts that are reasonable under the circumstances to maintain its secrecy.¹⁰ Trade secret protection is not automatic; the owner bears an affirmative duty to actively safeguard the information's confidentiality. And the owner has no claim if a competitor simply reverse engineers the trade secret using lawfully acquired information – without, for example, conspiring to obtain it from a person who has an obligation to keep that information confidential.¹¹ For a competitor to gain access to this information under “improper means” (theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means)¹² offends the basic principles of unfair competition law, which prevents a defendant from “reaping[] where it has not sown.”¹³

Federal law recognizes the national economic and security interests that trade secrets implicate. First, the Economic Espionage Act of 1996 (EEA) (18 U.S.C. § 1831 et seq.) creates criminal liability when the defendant steals a trade secret with the knowledge or intent that the offense will benefit any foreign government, foreign instrumentality, or foreign agent.¹⁴ The focus on *foreign government beneficiaries* distinguishes the EEA as a critical tool in combating state-sponsored economic warfare. Second, the EEA criminalizes the intentional theft of trade secrets for

⁸ [Uniform Trade Secrets Act \(UTSA\)](#) §§ 1–12 (Unif. L. Comm’n 1985).

⁹ UTSA § 1(4)(i).

¹⁰ UTSA § 1(4)(ii).

¹¹ UTSA § 1 cmt.

¹² UTSA § 1(1).

¹³ *Int’l News Serv. v. Associated Press*, 248 U.S. 215, 239 (1918). Trade secret law also protects against unauthorized use or disclosure by those who knew or had reason to know that information was derived from someone who used improper means, acquired it under circumstances giving rise to a duty to maintain secrecy, or knew it was acquired by accident or mistake. UTSA § 1(2) (defining “Misappropriation”).

¹⁴ 18 U.S.C. § 1831(a); see Economic Espionage Act of 1996, Pub. L. No. 104–294, § 101, 110 Stat. 3488–91.

general commercial or economic advantage, regardless of foreign government involvement.¹⁵ In both cases, Congress has made clear that it wishes to extend jurisdiction to its maximum reach: the statute applies if any portion of the illegal activity occurs in the United States.¹⁶

In 2016, the Defend Trade Secrets Act of 2016 (DTSA) created a federal civil cause of action for trade secret misappropriation.¹⁷ DTSA allows trade secret owners to file suit in federal court, provided the trade secret is related to a product or service for use in interstate or foreign commerce.¹⁸ By establishing a uniform federal standard and providing access to federal courts, DTSA complements state law protections and facilitates more consistent civil enforcement of trade secret rights across state lines.¹⁹

B. International Protection of Trade Secrets

The United States has robust enforcement mechanisms for trade secret law, and the definitions used in our laws are recognized in international agreements. Thanks to leadership across both parties, the United States led the adoption of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) into the General Agreement on Tariffs and Trade in 1994.²⁰ TRIPS establishes a crucial minimum standard for trade secret protection that all WTO member countries must implement within their national legal systems, fostering a more harmonized global landscape for safeguarding confidential business information.²¹

Article 39(2) of the TRIPS Agreement explicitly requires member countries to protect trade secrets (in the language of TRIPS, "undisclosed information"). To qualify for

¹⁵ See 18 U.S.C. § 1832(a).

¹⁶ See 18 U.S.C. § 1837(2).

¹⁷ 18 U.S.C. § 1836; see Defend Trade Secrets Act of 2016, Pub. L. No. 114–153, §§ 1–7, 130 Stat. 376–86.

¹⁸ 18 U.S.C. § 1836(b)(1).

¹⁹ See 18 U.S.C. §§ 1836, 1839.

²⁰ See Catherine Field, [Negotiating for the United States](#), The Making of the TRIPS Agreement, at 129–157 (WTO iLibrary 2015).

²¹ TRIPS incorporates an older international instrument, the Paris Convention for the Protection of Industrial Property—first adopted in 1883 and later amended in 1967 to include "unfair competition." Paris Convention, Art. 10bis. The TRIPS requirement to protect trade secrets exists for the express purpose of "ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967)." [TRIPS, Art. 39\(1\)](#).

protection under this article, information must meet three criteria, closely paralleling the UTSA definition: (i) it must be secret in the sense that it is not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (ii) it must have commercial value because it is secret; and (iii) it must have been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.²² Article 39(2) provides a mechanism to prevent qualifying undisclosed information from being disclosed to, acquired by, or used by others without their consent "in a manner contrary to honest commercial practices."²³ This phrase, "a manner contrary to honest commercial practices," may be compared to the "improper means" in United States law,²⁴ and is defined to include "breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition."²⁵

C. Application to AI: Safeguarding Innovation

Many of the most valuable assets generated during AI development are prime candidates for trade secret protection. These include:²⁶

- **Algorithms:** The core mathematical models, unique architectures, and processing logic that drive AI systems. Novel algorithms conferring a significant performance advantage are frequently maintained as closely guarded secrets.²⁷
- **Training Data:** The models are only as good as their training data. The significant investment required to design, clean, and curate high-quality

²² TRIPS, Art. 39(2)(a)–(c).

²³ TRIPS, Art. 39(2).

²⁴ Jorge Contreras, [Trade Secrets](#), Global Dictionary of Competition Law, Concurrences, Art. No. 85884 (discussing misappropriation under UTSA and TRIPS, Art. 39).

²⁵ TRIPS, Art. 39(2), n.10.

²⁶ See John Villasenar, [Artificial Intelligence, Trade Secrets, and the Challenge of Transparency](#), 25 N.C.J.L. & Tech. 495, at 508 (2024); Katarina Foss-Solbrekk, [Three routes to protecting AI systems and their algorithms under IP law: The good, the bad and the ugly](#), 16 J. Intell. Prop. L. & Prac. 247, at 247–258 (March 2021); U.S. House of Representatives Bipartisan Artificial Intelligence Task Force, [Bipartisan House Task Force Report on Artificial Intelligence](#) (Dec. 2024).

²⁷ See Zachary Brown, Peter Slattery, & Haoran Lyu, [What drives progress in AI? Trends in Algorithms](#), FutureTech (May 20, 2024).

datasets, and the unique insights derived from them, often render datasets themselves valuable trade secrets. The value lies not just in the raw data, but in its specific selection, annotation, organization, and quality.²⁸

- **Training Methodologies:** The specific techniques, parameters, hyperparameter tuning processes,²⁹ network configurations, and workflows employed to effectively and efficiently train AI models represent valuable know-how that can be protected.³⁰
- **Negative Know-How:** Information regarding failed experiments, unsuccessful approaches, and dead ends encountered during research and development. This "negative" information can be highly valuable, saving others time and resources by steering them away from unproductive paths.³¹

AI developers often strategically prefer to rely on trade secret protection rather than patents for several compelling reasons. Obtaining a patent requires extensive public disclosure of the invention, which is undesirable if confidentiality provides a more significant commercial edge. Trade secret protection arises automatically upon the creation of qualifying information and the implementation of reasonable secrecy measures. Additionally, trade secret law can protect broader categories of

²⁸ See generally Global Partnership on AI, Data Governance Working Group, [The Role of Data in AI: Report for the Data Governance Working Group of the Global Partnership of AI](#) (Nov. 2020); Katarina Foss-Solbrekk, [Three routes to protecting AI systems and their algorithms under IP law: The good, the bad and the ugly](#), 16 J. Intell. Prop. L. & Prac. 247, at 247–258 (March 2021).

²⁹ Hyperparameter tuning involves optimizing the model's learning such as the learning rate, the number of neurons in a neural network, or the kernel size in a support vector machine. (A Support Vector Machine in turn, is a supervised machine learning algorithm used for classification and regression tasks.) Unlike model parameters, which are learned from the data during training, hyperparameters are set before the training process begins and significantly impact the model's performance. See generally Sayak Paul, [Hyperparameter Optimization in Machine Learning Models](#), Datacamp.com (Aug. 15, 2018).

³⁰ Cong. Rsch. Servs., [Artificial Intelligence: Background, Selected Issues, and Policy Considerations](#), R46795 (May 19, 2021).

³¹ Animesh Giri, Jacob Pastor, & Laurence Freed, [Trade Secret Valuation in IP Disputes: Economics of Negative Information](#), ABA Bus. L. Section (Aug. 10, 2023) (discussing lawsuit between Waymo and Uber involving Uber's alleged theft of negative information and dead-end designs).

information, including valuable datasets and compilations, that might not meet the criteria for patentability.³²

However, the very nature of AI assets presents unique challenges for trade secret protection. With rare exception, they exist in digital forms that can potentially be copied and transmitted rapidly if security measures are breached, whether through external cyberattacks, insider threats, or other means.

III. Trade Secret Theft by the PRC is Unfair Competition

The theft of American IP jeopardizes all American economic efforts, from the development of AI technologies to support for small businesses. China's cyber-enabled IP theft is systematic, large-scale, and closely aligned with its national development goals. The proliferation of AI technologies is likely to accelerate both the scope and impact of these campaigns, threatening U.S. economic competitiveness and national security.

The common figure cited is that Chinese IP theft costs Americans \$225-600 billion annually, but this number is out of date. It comes from a USTR report in 2017,³³ before the proliferation of large language models (LLMs) and other cutting edge AI on which Chinese thefts have been especially aggressive.³⁴ China's preeminent LLM, DeepSeek-R1, was almost certainly built by stealing and distilling the products of American AI firms.³⁵ "Distillation" may refer to a range of practices including systematic querying and insertion of other outputs as well as direct use of code. DeepSeek used some data from OpenAI; it is unclear what data they used and how. OpenAI has terms of use for its data which they allege DeepSeek has violated. Testing of DeepSeek-R1 suggests that this use was illicit, as publicly available tests note both that responses from R1 were "almost identical to GPT-4" and that at

³² See Katarina Foss-Solbrekk, [Three routes to protecting AI systems and their algorithms under IP law: The good, the bad and the ugly](#), 16 J. Intell. Prop. L. & Prac. 247, at 256-258 (March 2021).

³³ USTR, ["2017 Special 301 Report"](#) (2017)

³⁴ See Benjamin Jensen, [How the Chinese Communist Party Uses Cyber Espionage to Undermine the American Economy](#), Statement Before the House Subcommittee on Courts, Intellectual Property, and the Internet (Oct 19, 2023) (describing the development of this strategy).

³⁵ Cade Meta, [OpenAI Says DeepSeek May Have Improperly Harvested Its Data](#), The New York Times (Jan 29, 2025).

various points when queried, R1 responded "I am also a version of ChatGPT, specifically based on GPT-4."³⁶

The pattern of Chinese IP theft has grown more brazen. The Department of Justice recently charged former Google employee Leon Ding, who allegedly stole trade secrets for the Chinese government and worked for two Chinese technology firms.³⁷ Google's report on adversarial misuse of AI also notes that more than 20 different PRC backed groups have attempted to misuse their LLM. In one case, a PRC-backed actor queried Gemini itself in an attempt to steal trade secrets on Gemini's architecture.³⁸ Chinese actors have also attempted to use Gemini to conduct research on US intelligence personnel, internet service providers, and the US military to locate targets and to compose messages for spear phishing attacks against these targets. OpenAI notes similar patterns of activity using ChatGPT noting that likely Chinese-backed threat actors used ChatGPT to "feed real time reports about protests in the West to Chinese security services" and "debug code."³⁹

And large companies are not the only ones in the PRC's crosshairs: A review of the Small Business Innovation Research (SBIR) program found that "nearly all" of the recipients the review sampled were targeted by the Chinese government.⁴⁰ Smaller AI startups are particularly vulnerable, as they will lack the resources to be able to detect and defend against state-sponsored incursion.

The United States still has some critical advantages over China in AI development, especially in developing new models. The most significant advantage is in computing power. CSIS projects that, by the end of 2025, the United States will have 14.3 million AI accelerator units to China's 4.6 million;⁴¹ US-based models continue to scale up computer power, across the 100K GPU barrier and now looking towards the 300K and 500K barriers. This has been supported by export restrictions on high-end

³⁶ OpenAI Developer Community Message Boards, [Is DeepSeek a Distilled Version of GPT-4? Analyzing Suspicious Behavior](#) (Jan 31, 2025).

³⁷ [Superseding indictment in United States v. Linwei Ding](#), a.k.a. Leon Ding, Case No: 24-cr-00141 VC (Feb 4, 2025).

³⁸ Google Threat Intelligence Group, [Adversarial Misuse of Generative AI](#), Google Cloud (Jan. 29, 2025).

³⁹ OpenAI, [Disrupting malicious uses of our models: an update](#), at 7. (Feb. 2025).

⁴⁰ Charles Wessner and Sujai Shivakumar, [Renew SBIR, Just Defend the Recipients against China](#), Center for Strategic & International Studies (CSIS) (Sept 2022).

⁴¹ Barath Harithas, [Securing the AGI Laurel: Export Controls, the Compute Gap, and China's Counterstrategy](#), CSIS (Dec. 20, 2024).



semiconductors and will likely be further supported by developments in domestic semiconductor manufacturing and data center development.

DeepSeek-R1 reflects China's approach to countering that advantage, including evading those trade restrictions.⁴² R1 received public attention because it produced results comparable to those of its American competitors with lower levels of computing power. China has to work with less computing power. As a result, stealing and distilling American products is a way of hijacking the computing work done to build the American products. Recent studies of AI products suggest that the United States still has a lead in model performance, but China has made significant progress in closing the gap.⁴³

As discussed above, the means of theft by the PRC and PRC-sponsored organizations can take many forms. Rapid technological change in the fields of cybersecurity and AI exacerbate challenges protecting critical trade secrets. The proliferation of sophisticated cyber threats and the complexities of managing information across distributed networks demand correspondingly sophisticated technical, contractual, and physical security protocols.

The Chinese threat actor Salt Typhoon, for example, perpetrated one of the largest intrusions into US telecommunications infrastructure in history, and a recent report from Gladstone suggests data center infrastructure built to support AI development is exposed to Chinese attacks.⁴⁴ Both examples highlight an ongoing need to secure infrastructure used to create AI products. These products are financially and strategically valuable.

Our members' networks are tested by state actors every day, and maintaining their security is a constant challenge. When those measures are breached, remedies can be difficult to come by, and defendants will try to play by two sets of rules. For example, U.S. courts have rejected attempts by a Chinese defendant to refuse to disclose information in discovery due to privacy restrictions in Chinese law.⁴⁵ In

⁴² Xingui Kok, [Singapore charges three with fraud that media link to Nvidia chips](#), Reuters (Feb. 28, 2025).

⁴³ For recent discussion, see Stanford HAI report. Re: number of models at page 49. Re: performance metrics at page 64. Stanford Human-Centered AI (HAI), [Artificial Intelligence Index Report 2025](#) (Jan. 2025).

⁴⁴ Jeremie Harris and Edouard Harris, [America's Superintelligence Project](#), Gladstone AI (Apr. 2025).

⁴⁵ [Cadence Design Systems, Inc. v. Syntronic AB et al.](#), No. 21-cv-03610-SI, 2021 WL 4222040, Dkt. 52 (N.D. Cal. Sept. 16, 2021).



contrast, an American company facing trade secret theft in China faces several hurdles. First, proving trade secret theft is difficult: unlike in the United States, China does not have a civil discovery process. There are no mechanisms for things that American lawyers would find commonplace: broad interrogatory and document requests, pretrial depositions, and even safeguards against evidentiary spoliation.⁴⁶ And despite a separate agreement signed in 2020 with the United States⁴⁷ and a WTO dispute that China settled in 2022 with the EU,⁴⁸ the USTR's 2025 section 301 report concluded that enforcement of trade secret law by the Chinese government continues to be "weak" and "China needs to address concerns regarding the risk of unauthorized disclosures of trade secrets and confidential business information by government personnel and third-party experts, which continue to be a serious concern for the United States and U.S. stakeholders in industries such as software, manufacturing, and cosmetics."⁴⁹

Both China and the United States are increasing the number of AI products produced every year. China's ability to reduce the computing demands and cost of building models has resulted in a significant increase in the number of frontier models. As this race tightens and the US builds larger manufacturing and computing infrastructure to support the development of AI, we also need to ensure that infrastructure is secure against intrusion, espionage, and sabotage.

IV. What Can Congress Do?

Congress has addressed substantive rights governing trade secrets in the United States and international law, developed through the combined efforts of the United States government and its trading partners, including China, have developed a global framework to respect those rights. The existence of adequate legal protection is not the problem. What is lacking is a means to sufficiently incentivize the Chinese government to abide by those protections or to provide means to enforce those protections. While there is no perfect solution, Congress has tools that it can and

⁴⁶ See generally Andrea Jeffries et al., [A Primer on Chinese Trade Secrets Disputes for U.S. Practitioners](#) (2024); USPTO's Silicon Valley IP Roadshow, Charles Graves, [Basics of Trade Secret Law and Enforcement in China](#) (2017).

⁴⁷ [Economic and Trade Agreement Between the Government of the United States of America and the Government of the People's Republic of China](#) (Jan. 15, 2020).

⁴⁸ *China – Enforcement of Intellectual Property Rights*, WTO Doc. WT/DS611 (Panel established Feb. 27, 2023).

⁴⁹ USTR, [2025 Special 301 Report](#), at 45, 46 (Apr. 29, 2025).



should develop to further protect American AI development from foreign theft and possibly sabotage.

We would suggest four areas for Congressional attention.

The first is cybersecurity: building and updating infrastructure to keep up with emerging and evolving threats is a constant project. Large technology companies are constant targets and face threats every day; they build up cutting-edge cybersecurity systems to protect their products and users. Successful espionage operations against large companies create high profile stories, but many attacks target smaller companies who do not have the same cybersecurity resources as our larger members.

The government should therefore continue to develop and expand resources made available to small businesses, who lack the funds to build their own cybersecurity resources. Government programs oriented towards small businesses, including SBIR and STTR, are helping companies innovate. We need to ensure that, as they innovate, their intellectual property is protected and not just stolen by the Chinese. The Cybersecurity for Small Business Pilot Program⁵⁰ is a start, and using grants and resources can protect American innovation.

Second, Congress should ensure that the scope of the CFIUS process continues to serve as an effective way to address trade secret risk.⁵¹

Third, Congress should assist the Administration in working with our allies and partners to build AI infrastructure on trusted providers. Adoption of Huawei and other PRC-located providers creates an unreasonable potential for trade secret theft.

Finally, while the legal framework for protecting trade secrets is well-developed, an emerging area of concern involves the potential exploitation of the U.S. legal system itself to gain unauthorized access to sensitive proprietary information through third-party litigation funding (TPLF) in patent disputes.⁵²

The broad scope of discovery available in U.S. litigation can provide an asymmetric advantage to a state actor. For example, discovery requests in a patent case are

⁵⁰ Small Business Administration, [SBA Awards \\$3 Million in Cybersecurity Pilot Program Grants](#) (Sept 20, 2024).

⁵¹ U.S.-China Economic and Security Review Commission (USCC), [Annual Report to Congress](#), at 174-182 (Nov. 2024); Sean O'Connor, [How Chinese Companies Facilitate Technology Transfer from the United States](#), USCC (May 6, 2019).

⁵² Donald J. Kochan, [Keep Foreign Cash Out of U.S. Courts](#), Wall Street Journal (Nov. 24, 2022).



often broad enough to cover even trade secrets related to the products involved—even when those trade secrets cannot be the subject of the relevant patents. A well-funded litigant, particularly one backed by an undisclosed third party with strategic interests beyond the case itself could potentially exploit the discovery process through overly broad or targeted requests aimed specifically at extracting trade secrets or other sensitive competitive information. And if that litigation is funded by a state actor (as has been documented to have happened), trade secrets are at high risk.⁵³ Congress possesses authority to mitigate this risk by mandating greater transparency in litigation funding, especially concerning funding originating from foreign sources. Transparency in this context would ensure that federal judges have the ability to craft appropriate protective orders.

As a final note, we would caution Congress against mandating detailed disclosure of AI training data sets. SIIA supports allowing courts to determine when and how to disclose details about training data, techniques, and approach. In the cases where content owners have filed lawsuits against AI companies based on the training of the AI models, courts are well equipped to determine what information should be shared and how it should be protected during litigation. The critical need is ensuring that there is no foreign entity behind the litigation using it to improperly uncover the key technologies of American AI companies. Additional transparency rules around training AI data are not required because the courts are equipped to determine how much disclosure should be required in any given case, and an overbroad approach could result in the disclosure of trade secret information.

V. Conclusion

The landscape around AI and intellectual property is constantly evolving, and as technology advances new threats emerge. That pattern is unlikely to stop in the near future, and we commend the Subcommittee for continuing to monitor these issues and engage industry. Thank you for your consideration of our views, and we are happy to serve as a resource.

⁵³ See e.g., U.S. Chamber of Commerce, [A New Threat: The National Security Risk of Third Party Litigation Funding](#) (2022); GAO, [Intellectual Property: Information on Third Party Litigation Funding of Patent Infringement](#), at 15 (“Stakeholders noted examples of several countries with involvement in funding patent litigation, including China, Saudi Arabia, and France, but did not know the extent of this funding given the limited available data.”).

Mr. ISSA. Thank you. Ms. Toner.

STATEMENT OF HELEN TONER

Ms. TONER. Chair, Ranking Member Johnson, Ranking Member Raskin, and the Members of the Subcommittee, thank you for the opportunity to testify.

My name is Helen Toner and I'm part of the founding team at CSET, the Center for Security and Emerging Technology at Georgetown, where for the past six years I've focused on AI and national security, U.S.–China competition over AI, and AI safety and security issues, more broadly.

It's a cliché that AI is hard to govern because the technology is moving so fast, but there's one important thing about AI that is actually quite predictable: It's only getting more capable, more powerful, and more strategically critical.

This is especially true of what gets called frontier AI systems, which are the focus of my testimony. Frontier AI is a term for the most cutting-edge general purpose AI systems, like Google's Gemini 2.5, OpenAI's o3, or Anthropic's Claude 3.7.

The companies at the AI frontier are actively working to build so-called artificial general intelligence, or AGI, which, roughly, means AI that is as smart as a human, or even to build super intelligence, which is AI far more capable than a human. The CEOs of these companies claim that they'll get this far within the next 2–5 years. It is not just marketing hype; many top researchers agree.

Even if 2–5 years is overly optimistic, the possibility that major tech companies could build human-level AI anytime in the foreseeable future should galvanize us to take action now. What action?

If we agree that AI is of strategic importance is already high and will only grow from here, I want to note two vital national security interests that follow from that.

First, for the topic of this hearing, the U.S. Government has a critical national security interest in protecting the trade secrets and IP of leading U.S. AI companies.

Second, there's also a critical national security interest in understanding and monitoring the development of frontier AI as it moves toward AGI and even super intelligence.

The most important point I want to make today is that these two critical priorities—security and transparency—do not need to be in tension with one another. We can pursue both in parallel.

My written testimony lays out the kinds of trade secrets that are most important to protect, primarily AI models themselves, as well as the algorithmic secrets used to create them, and datasets, and hard regulated IP as well.

I also lay out the areas where we most need transparency. These are things like testing for capabilities and risks of new systems; the goals that AI models are trained to pursue; safety and security risk management practices within the frontier AI; data on their internal use of AI, and whistleblower protections for their employees.

Notice that there's not much overlap between the things we most need to keep secure and the things that we most need to bring into the sunlight. Where overlap does exist, we have options. Information can be shared with governments via secure channels, or it

could be shared only with third-party independent auditors who work under NDA inside companies' own facilities.

I would make the following five recommendations to this Subcommittee and to Congress:

First, fund and expand security collaborations between the U.S. Government and frontier AI companies. There are several small-scale voluntary programs that have recently been started, including threat intelligence-sharing with the intelligence community and voluntary testing for capabilities that are relevant to national security. These initiatives are highly valuable and should be strengthened and expanded.

Second, on transparency, you can use existing authorities or create new ones to increase visibility into the most advanced AI systems being built by frontier companies. Many of these companies have already made voluntary commitments to share safety and security information. So, Congress can ask them about how those commitments are going and make sure they're fulfilling them reliably. There are also existing authorities that the government can use to compel disclosure, if necessary. New legislation could enshrine transparency requirements targeted for AI or create whistleblower protections for AI company employees.

Third, invest in the technologies and infrastructure that we need to ensure that strategically critical AI systems of the future stay secure. This could include R&D funding, public-private partnerships, or demonstration projects that push forward things like secure-by-design hardware or highly secure data centers.

Fourth, consider giving companies permission to prioritize security in ways that are currently legally fraught. One example here is creating safe harbor from antitrust concerns, specifically, for collaboration on safety and security issues. Another possibility would be to enact legislation that makes it easier for AI companies to engage in intensive personnel vetting and monitoring to reduce insider threats.

Fifth, in your interactions with AI companies, press them on what their cybersecurity practices look like and how they're working to improve. Use your bully pulpit to impress on them that this is a critical question of U.S. security and competitiveness. The United States cannot lead if adversaries have easy access to our best technology.

Thank you and I look forward to your questions.

[The prepared statement of Ms. Toner follows:]

*Testimony before the U.S. House Committee on the Judiciary, Subcommittee on Courts,
Intellectual Property, Artificial Intelligence, and the Internet*

For the hearing titled

"Protecting Our Edge: Trade Secrets and the Global AI Arms Race"

May 7, 2025

Helen Toner

*Director of Strategy and Foundational Research Grants
Center for Security and Emerging Technology, Georgetown University*

Chair Issa, Ranking Member Johnson, members of the Subcommittee: Thank you for the opportunity to testify before you today.

I have spent the last 6 years working on AI and national security policy at Georgetown University's Center for Security and Emerging Technology (CSET). U.S.-China competition in AI is a major focus of my research, as are questions of AI safety, security, and governance. I served on OpenAI's board of directors from 2021 to 2023.

Context and Focus

My testimony will focus on trade secrets and competition issues relevant to so-called "**frontier AI**," which refers to cutting-edge, general-purpose AI systems such as Google's Gemini 2.5, OpenAI's o3, Anthropic's Claude 3.7, xAI's Grok 3, and Meta's Llama 4.

Frontier AI is only one part of the larger AI ecosystem, but from a strategic perspective, it is an especially important part. The companies at the frontier are actively working to build artificial general intelligence (AGI), i.e. AI that is as capable as human experts across a wide range of fields. The CEOs of these companies claim that this goal will likely be reached within the next 2-5 years,¹ a view shared by top researchers and engineers both inside and outside of these companies. Once they reach AGI, they plan to push ahead with building "superintelligence," i.e.

¹ [Anthropic CEO Dario Amodei](#): "Making AI that is smarter than almost all humans at almost all things [...] is most likely to happen in 2026-2027." [OpenAI CEO Sam Altman](#): "I think AGI will probably get developed during this president's term." [Google DeepMind CEO Demis Hassabis](#): "I think we're probably three to five years away [from AGI]."

AI that is far smarter and more capable than humans.² Even if their projected timelines are overly optimistic, it is not an exaggeration to say that this level of AI would reshape the economy, upend the political system, and transform the international order.

The idea that AI is hard to govern because the technology is moving so fast is clichéd, but true. But how AI is changing is predictable in at least one important way: it is getting more capable, more powerful, and more strategically critical.

Within the scope of this hearing, this has two important implications:

- **The U.S. government has a critical national security interest in protecting the trade secrets and IP of leading U.S. AI companies.**
- **The U.S. government has a critical national security interest in understanding and monitoring the technology being built inside leading U.S. AI companies.**

These two interests do not need to be in tension with each other, and can be pursued in parallel. I elaborate on how below.

The Importance of Securing Frontier AI Companies

As leading AI companies' technology becomes increasingly strategically sensitive, the national security implications of inadequate cybersecurity grow more acute than for a typical company. If we believe that it's vitally important for the world's most advanced AI systems to be developed and deployed by U.S. companies, then we must also believe that it's vitally important to prevent that AI technology from being stolen by our adversaries.

Unfortunately, current security practices at leading AI companies are insufficient to prevent compromise by advanced persistent threat (APT) actors such as state-based cyber operations. Even the best-defended companies in America are widely acknowledged to be unable to resist penetration by APTs, and AI companies are no exception. In most sectors, this vulnerability entails risks to U.S. citizens' personal data and companies' commercially sensitive IP. As AI advances, the stakes for frontier AI companies grow even higher than this—more akin to threats to critical infrastructure providers or companies in the defense industrial base. Compromise of a frontier AI system, theft of key trade secrets involved in creating it, or even the wholesale exfiltration of a frontier model itself would seriously harm U.S. prospects in the global AI competition, with implications for future military competitiveness, economic competitiveness, and national power more broadly.

² E.g. per [Sam Altman](#): "We are beginning to turn our aim beyond AGI, to superintelligence in the true sense of the word."

What's more, we know that foreign actors (including but not limited to China and Russia) are extremely capable of stealing U.S. intellectual property and extremely interested in boosting their domestic AI ecosystems.³ This means that the leading U.S. AI companies are sitting ducks for major state-sponsored operations to steal critical trade secrets that could eat away at U.S. AI leadership.

One way of breaking down the trade secrets of concern in frontier AI development is to consider AI models themselves, plus the [triad](#) of inputs used to make them: algorithms, data, and hardware.

- **AI models** are frontier AI companies' crown jewels. To steal a model, the attacker needs to download a file containing the set of numbers known as "model weights" or "parameters." For today's leading models, this file is likely on the order of several terabytes in size, meaning exfiltration is non-trivial but possible. If an adversary is able to steal a trained model, they have access to the capabilities of that model without needing the world-class team, months of research time, and tens or hundreds of millions of dollars used to create ("train") the model. They can also flexibly modify or further build on the model. For these reasons, the weights of frontier models are broadly considered the highest priority type of intellectual property for frontier AI companies to protect.
- **Algorithmic secrets** is an overarching term used to describe privately held insights and techniques used to design and train models. They include model architectures (the design of the model), training "recipes" (the sequence of steps used to optimize the model), nuggets of practical know-how, and new research ideas. Algorithmic secrets often take the form of a few sentences—perhaps a single sentence—that could be extracted from internal documents or messaging platforms, or even let slip by an incautious employee.
- **Training datasets** are the data used to create AI models. For frontier AI models, these include multi-trillion-word corpora of text and other data scraped from the internet and other sources; carefully curated human-written examples of priority use cases; collections of human-submitted or AI-generated rankings and ratings comparing different AI-generated options; AI-generated text; and other types of data.
- **AI hardware** provides the computing power (often referred to as "compute") needed to train frontier models. Access to state-of-the-art AI chips, which are subject to U.S. export controls, is a major competitive advantage for U.S. frontier AI firms. The most

³ See, e.g., Hannas, Mulvenon, and Puglisi 2013, *Chinese Industrial Espionage*.

sensitive trade secrets associated with AI hardware are chip designs, though these are of limited utility unless the thief can access leading-edge chip production facilities. In most cases, chip designs are not held by AI companies themselves, since almost all frontier AI companies use graphics processing units (GPUs) designed by NVIDIA. The exception is Google, which uses its in-house tensor processing units (TPUs). The GPUs and TPUs used for frontier AI training can currently only be produced by the Taiwanese Semiconductor Manufacturing Corporation (TSMC).

Trade secrets in these categories have already been stolen from top firms. In 2023, an attacker gained access to internal communication channels at OpenAI and was able to extract proprietary information on how they develop their AI technology, i.e. algorithmic secrets.⁴ In 2024, the FBI arrested a Google employee for systematically exfiltrating large volumes of confidential information from Google, including information relating to Google's TPU AI chips.⁵

A 2024 RAND analysis found that there were many areas where frontier AI companies could immediately improve their security, and that there was also a need for significant investments over the longer term to increase their capacity to resist more sophisticated attacks.⁶

The Importance of Government Visibility Into Frontier AI Development

U.S. frontier AI companies claim that they are on track to build extraordinarily powerful—and potentially extraordinarily dangerous—technology in the next 2-5 years. Materials produced by frontier AI companies describe a range of severe risks that their own AI systems might soon pose, including aiding in sophisticated offensive cyber operations, enabling amateurs to carry out bioterror attacks, and potentially evading human control entirely.⁷ Even in scenarios where all goes to plan and these catastrophic risks do not materialize, increasingly advanced AI will have extremely disruptive effects on society more broadly.

Historically, technologies with such major strategic implications have been developed under the auspices of the U.S. government and closely associated firms. This time, it is being developed entirely within private industry, with little visibility available to Congress or the executive branch. This threatens the U.S. government's ability to appropriately manage and

⁴ [New York Times 2024](#), "A Hacker Stole OpenAI Secrets, Raising Fears That China Could, Too."

⁵ [Department of Justice 2024](#), "Chinese National Residing in California Arrested for Theft of Artificial Intelligence-Related Trade Secrets from Google."

⁶ [Nevo et al. 2024](#), "Securing AI Model Weights."

⁷ See Anthropic's [Responsible Scaling Policy](#), OpenAI's [Preparedness Framework](#), and Google's [Frontier Safety Framework](#).

respond to continued developments in frontier AI, up to and including the possible development of AGI and superintelligence.

Efforts to develop a robust regulatory framework for frontier AI have largely stalled out at the federal level in the United States. In the absence of such a framework, there is broad agreement among AI policy experts with widely varying political views that transparency and disclosure requirements are a minimal, light-touch approach that should be pursued.⁸ Increasing the information flow between frontier companies and the outside world has a slew of benefits—it reduces information asymmetries, empowers government to understand and respond to advances, and equips the public to weigh in on a technology that will profoundly impact them.

Transparency requirements for AI development can take different forms, depending on the information of interest and the tradeoffs involved in sharing it. Three major types of transparency are disclosure to the *public*, disclosure to *government*, and disclosure to a *third-party auditor*. Each of these balances different pros and cons. Public disclosure goes furthest in reducing information gaps, but may be undesirable for information that is sensitive from a commercial or national security perspective. Disclosure directly to USG is well suited for information directly related to national security, such as results of tests on AI models' capabilities in areas including cyber operations, bioweapon development, and nuclear weapons. Disclosure to third-party auditors is a flexible option that can allow a neutral, independent organization to verify or assess sensitive information while keeping it largely under the AI company's control, e.g. by having the auditor work within the AI company's own facilities under a non-disclosure agreement.

Forcing U.S. companies to disclose information that would damage their competitiveness would not be a good approach. Fortunately, most of the information that is of greatest interest from a national security and public interest perspective would not damage competitiveness if disclosed appropriately. Types of information that would be valuable to share include:

- **Results of testing for AI models' capabilities and risks.** A lack of clear, up-to-date information about what the world's best AI systems are capable of puts the U.S. government at a huge disadvantage in understanding how the AI frontier is progressing and what kinds of responses might be needed. At present, information about how rapidly AI is advancing is shared (or not shared) at the discretion of companies, on the timeline and in the format that they find most convenient.

⁸ See, e.g., [Ball and Kokotailo 2024](#), "4 Ways to Advance Transparency in Frontier AI Development."

- **Information about the goals or specifications AI models are being trained to pursue.**
This creates visibility into how companies are making crucial, politically loaded decisions about what their models should and shouldn't do, as well as how to prioritize different values (e.g. freedom of speech vs. avoiding hate speech, supporting users vs. avoiding sycophancy, etc.). As frontier AI models are integrated into citizens' lives, businesses' software, and government's infrastructure, knowing what they are designed to optimize for will become increasingly important. [OpenAI](#) and [Anthropic](#) voluntarily share a version of this information, to their credit.
- **Analysis of why AI developers believe their current risk management practices are sufficient** (sometimes referred to as a [safety case](#)). Developing and releasing frontier AI models involves making a large number of judgment calls about how to test for risks, what results are acceptable, and how to manage uncertainty. Making at least a high-level version of that thinking transparent to a wider audience (perhaps with especially sensitive details redacted) would bring these critical decisions out from closed meeting rooms into the sunlight.
- **Data on internal usage of AI.** Frontier AI companies are increasingly relying on their own, sometimes unreleased, AI models to automate their own work. It is a widely held view among AI researchers and CEOs that using AI to accelerate AI research could lead to a runaway feedback loop of increasingly advanced AI. Such a feedback loop is known as an "intelligence explosion," and is at the center of some of AI experts' greatest fears about AI catastrophe. Greater transparency about the extent to which AI is in fact accelerating research would prevent this phenomenon from transpiring in secret.
- **Whistleblower reports.** If AI companies want to claim that they are building the most world-changing technology to ever exist, their employees should be able to share concerns about risks to public safety along the way without fearing the repercussions. AI whistleblowing is largely unprotected by existing whistleblower laws, which focus on outright illegal activity.

Note how little these categories overlap with the trade secrets outlined in the previous section. The categories immediately above are areas where the public or governmental interest in transparency is much higher than the downside of making the information available to competitors. This cost-benefit is different for other types of information. In particular, as outlined in the previous section, information about how AI models are built (e.g. architectural details, training recipes, or full datasets) is more commercially sensitive, as are the models themselves.

In weighing the pros and cons of requiring any particular kind of information be disclosed, however, it is important to recall that even commercially sensitive information is already stored inside AI companies themselves, where it is already vulnerable to espionage. This baseline should be considered alongside the sensitivity of the information, the benefit of sharing it, and the security of where it would be stored (e.g. in a classified USG environment vs. on a public website).

Recommendations

There are a range of actions available to Congress, in its legislative and oversight capacities, to pursue the twin priorities of keeping U.S. frontier AI secure while ensuring visibility into its development:

1. **Expand and resource security-focused collaborative arrangements between the U.S. government and frontier AI companies.** Several small-scale, voluntary programs currently exist, such as threat intelligence sharing with the intelligence community and voluntary testing for national security-relevant capabilities at a dedicated institute within NIST. These initiatives are highly valuable and should be strengthened.
2. **Use existing authorities, or create new ones, to promote transparency from frontier AI companies about their most advanced systems.** Without new legislation, Congress can ask AI companies about their compliance with their own voluntary commitments to share safety and security information. The U.S. government can also use existing authorities, such as the Defense Production Act, to require companies to share information via secure channels. In addition to these options, new legislation could enshrine transparency requirements and/or create whistleblower protections for AI company employees, for example by shielding them from retaliation, identifying clear channels to report concerns, and creating monetary incentives.
3. **Invest in the technologies and infrastructure needed to ensure the security of strategically critical AI systems of the future.** Confidential computing techniques could allow model weights to be kept secure at the chip level, even while in use, but would need to be adapted and adopted at scale. Federal funding could help accelerate the availability of this technology. Likewise, it may be necessary to rebuild advanced AI data centers from the ground up to maximize security; if so, public funding or public-private partnerships could be helpful.
4. **Consider creating legal space to allow companies to prioritize security in ways that are currently legally fraught.** One example would be creating safe harbor protections for companies to collaborate on AI safety and security issues without triggering

antitrust concerns. This would of course need to be structured in a way that would not permit collusion. Another possibility would be authorizing AI companies to engage in intensive personnel vetting and monitoring, practices that may be discouraged under state employment law but that would be essential in any serious effort against insider threats. Crucially, any personnel-focused efforts must be implemented thoughtfully in order to protect the enormous contributions of foreign nationals to U.S. AI competitiveness.⁹ What is needed is a scalpel—the ability to carefully identify individuals who should not have access to highly sensitive trade secrets, and keep tabs on those who do have access—not a sledgehammer of anti-immigrant measures.

5. **Push frontier AI companies to improve their cybersecurity practices**, and emphasize to them that this must be a high priority. Make clear that the security of critical frontier AI IP is as core to U.S. competitiveness as rapid innovation, since the United States cannot lead if adversaries have easy access to our best technology.

Thank you, and I look forward to your questions.

⁹ See [Zwetsloot 2021](#), “Winning the Tech Talent Competition,” and [Oschinski et al. 2025](#), “Strengthening America’s AI Workforce.”

Mr. ISSA. Thank you. Mr. Andersen.

STATEMENT OF NICHOLAS ANDERSEN

Mr. ANDERSEN. Mr. Chair, Ranking Member Johnson, Ranking Member Raskin, and the Members of the Subcommittee, thank you for the opportunity to testify today.

My name is Nick Andersen. I've served in senior cybersecurity leadership roles in the previous Trump Administration, including as the Principal Deputy Assistant Secretary and performing the duties of the Assistant Secretary for Cybersecurity, Energy Security, and Emergency Response at the Department of Energy. I've also served in White House—I was a White House cyber official, a State Chief Information Security Officer, and a Chief Information Officer in the intelligence community.

All that is to say I am not before you today as someone who can intensive IP legal analysis, but as a national security and cybersecurity professional who spent nearly two decades defending this country, often against the adversaries who are now racing to dominate the future of AI.

The Chief among them is the Chinese Communist Party. Almost as a mirror image, as we sit here, just last week Xi Jinping presided over a Politburo study session on AI. Let me be clear: The People's Republic of China does not simply seek to compete with us; it seeks to overtake us. In doing so, it's not going to be through fair market competition. It's going to be doing so through theft, deception, and the systematic targeting of America's innovation base. The tactics used by the Chinese intelligence services and the State-backed actors include cyber intrusions, insider recruitment, deceptive investment strategies, and the use of academic partnerships as cover for espionage.

This is not speculative. It is confirmed through multiple indictments by the Department of Justice and ongoing intelligence assessments from the Office of the Director of National Intelligence.

The AI community, particularly companies building dual-use technologies, have become a top target. Yet, our national defenses remain inconsistent. We do not require minimum security baselines for companies building next-generation models. We do not vet outbound investments that may expose sensitive technology. We do not hold venture capital or private equity firms accountable for facilitating access to strategic industries by foreign adversaries. This must change.

I support efforts to codify these outbound investment screenings, strengthen cyber requirements for federally funded tech firms, and require public disclosures when there's foreign ownership or influence in American AI companies.

This is not about isolationism; it's about discipline, strategic clarity, and the courage to act before it's too late. During our previous years in the last administration, we took bold steps to harden our infrastructure and disrupt adversary operations. This results-driven approach, including offensive cyber operations, must be returned.

I believe we have 2–5 years to close the most dangerous gaps. Beyond that, we risk losing our technological and strategic edge-

possibly for good. AI is not just an economic issue; it's a national security issue and we must treat it accordingly.

Thank you for the opportunity to speak today and I look forward to your questions.

[The prepared statement of Mr. Andersen follows:]

Written Testimony of Nicholas Andersen

Before the House Judiciary Committee

Subcommittee on Courts, Intellectual Property, and the Internet

Hearing: "Protecting Our Edge: Trade Secrets and the Global AI Arms Race"

May 7, 2025

Chairman Issa, Ranking Member Johnson, and distinguished members of the Subcommittee, thank you for the opportunity to testify on the urgent matter of protecting American trade secrets in the age of artificial intelligence (AI).

My name is Nicholas Andersen. I previously served as a senior cybersecurity official during the Trump administration, including as the Principal Deputy Assistant Secretary and Performing the Duties of the Assistant Secretary for the Office of Cybersecurity, Energy Security, and Emergency Response at the United States Department of Energy, in addition to my service in the White House, as a State Chief Information Security Officer (CISO) and Intelligence Community Chief Information Officer (CIO).

Today, I appear before you not as a legal expert as many of my colleagues may be, but as a national security and cybersecurity professional who has spent nearly two decades defending the United States against digital threats—many of them originating from the People's Republic of China (PRC). We are engaged in a global competition, and at its heart is the ability to secure and control the most advanced technologies of our time. Artificial intelligence is not merely an economic driver—it is a battlefield asset.

During the previous Trump administration, we delivered historic progress on securing critical energy infrastructure, elevating federal and private-sector collaboration, and taking unprecedented steps to disrupt cyber operations by adversaries. We prioritized real-world outcomes over bureaucratic exercises, and it worked. That results-driven approach must return again as we now commit again to outcomes rather than soundbites.

Unfortunately, over the past four years, we have watched strategic deterrence erode. Foreign adversaries face fewer consequences for targeting American innovation. Executive branch agencies have been more focused on process than protection. We must be prepared to act decisively and without hesitation to confront this threat.

The Chinese Communist Party (CCP) sees AI as a foundational element of its effort to supplant the United States as the global technological, economic, and military leader. Their strategy is not just to build capabilities domestically, but to extract, acquire, and steal them from us—through cyber-enabled theft, insider infiltration, and coerced transfer of technology. For China, innovation theft is not just tolerated—it is systematized, state-sponsored, and celebrated.

We must treat this for what it is: a sustained, government-backed assault on the American innovation base. The PRC is not operating as a competitor in good faith. They are leveraging their intelligence services, their state-owned enterprises, and even American legal and financial institutions to create openings for espionage and exploitation. And they are doing it in real time.

What makes the PRC threat uniquely dangerous is not just the scale of its cyber operations, but the strategic doctrine behind them. The CCP's Military-Civil Fusion policy erases any distinction between the private sector and the Chinese military. Their National Intelligence Law requires all citizens and entities to cooperate with state intelligence activities upon request. This means that any Chinese company interacting with American firms—whether through investment, supply chain participation, or joint research—is potentially an extension of the Chinese state.

In the cybersecurity community, we have long recognized that trade secret protection is only as strong as the defensive perimeter surrounding the data. Unlike patents, trade secrets are not protected by legal registration, but by the integrity of the systems, networks, and people that guard them. For this reason, cyber-enabled espionage is the single greatest threat to the long-term viability of American AI development.

The tactics used by the PRC and its proxies are wide-ranging: from remote intrusions targeting source code repositories and research institutions, to the use of joint ventures and academic exchanges as cover for data extraction. These efforts are deliberate, persistent, and operationally supported by the Chinese intelligence and military apparatus. It is not a matter of if they are targeting us—it is a matter of how deeply they have already penetrated key sectors.

From a national security standpoint, we must treat AI companies—especially those working in dual-use applications—as critical infrastructure. Their models, training data, and research pipelines are not just business assets; they are targets of foreign intelligence collection. Congress should act with urgency to prioritize cyber hardening measures across this sector. This includes developing minimum cybersecurity requirements for firms operating in designated strategic technology areas, expanding access to classified threat intelligence, providing incentives for robust secure-by-design practices, insider threat detection programs, and participation in classified or unclassified threat-sharing programs operated by the Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI).

Additionally, we must recognize that our adversaries do not only exploit our networks—they exploit our openness. American capital itself can be a vector for strategic vulnerability. Private equity and venture capital firms—many of which are headquartered in the United States—routinely fund startups or firms operating in critical technology sectors without fully understanding or disclosing the downstream national security risks. They become unwitting participants in China's acquisition strategy. Congress should move swiftly to codify outbound investment screening mechanisms, restrict engagement with entities affiliated with the CCP and the Chinese military, and to require public

disclosures of investments that involve AI or other sensitive technologies when there is a nexus to foreign ownership or influence.

We need a new doctrine for cybersecurity and AI—a clear, uncompromising framework built on American strength. It must include: zero taxpayer dollars for tech that strengthens China, no federal contracts without real standards for adequate cybersecurity, no more U.S. capital funding adversary-controlled firms, and a decisive offensive cyber posture to disrupt and dismantle threat actor infrastructure before harm occurs.

There is a narrative that stronger protections or tougher cyber requirements will somehow “slow down” innovation. I believe the opposite is true. Failing to protect what we build is what truly limits our future. American innovation thrives when our best minds and companies know their work will not be stolen, cloned, or militarized against them by a foreign regime.

I would caution this Subcommittee against overreliance on legal mechanisms alone. Laws and lawsuits do little good when the adversary operates outside our jurisdiction and beyond the reach of our courts. We need preemptive action, not passive defense. We must build resilient networks, promote real-time threat sharing, empower private sector defenders, and coordinate disruption efforts against foreign cyber actors. This must be a whole-of-government and whole-of-nation response.

The clock is ticking. Based on the pace of Chinese technology acquisition, the growing capabilities of its cyber operations, and the accelerating role of AI in defense and intelligence, I believe we have no more than two to five years to close the most dangerous gaps. Failing to act now will result in the permanent erosion of our technological and strategic advantage.

American companies developing AI systems are being targeted systematically. The tactics used by PRC-linked actors include cyber intrusions, insider recruitment, investment strategies meant to gain access to non-public information, and partnerships with academic institutions designed to extract sensitive research. Recent indictments by the United States Department of Justice (DOJ) and ongoing reporting by the ODNI confirm the breadth and sophistication of this campaign.

Protecting America’s AI future is not about isolationism or fear—it is about clarity, discipline, and courage. We must recognize that AI is not just a competitive industry: it is a foundation of national power. We must treat it accordingly.

Thank you for the opportunity to share my perspective. The United States cannot afford delay. We need leadership that understands this threat, has countered it firsthand, and will not hesitate to act. I stand ready to serve.

In the coming years, the United States must make a conscious decision about what kind of leadership it wants in the cyber domain. We can either remain on defense, reacting to breaches and intellectual property theft after the damage is done—or we can lead again.

Leadership means unapologetically defending American interests. It means re-establishing global norms through strength, not submission. It means calling out adversaries by name—especially the People's Republic of China—and holding them accountable with real costs, not symbolic gestures.

We need a return to the kind of decisive, disruptive cyber posture we began building in 2017. That includes stronger public-private partnerships, bold offensive capabilities, and the institutional will to act faster than our adversaries.

Thank you again for this opportunity to contribute to our national dialogue. I look forward to answering the questions of this Subcommittee as we seek to restore American strength in the digital age.

Mr. ISSA. Thank you.

We will now go back and forth between the majority and minority, beginning with the gentleman from Wisconsin.

Mr. FITZGERALD. Thank you, Mr. Chair.

Mr. Andersen, AI's infrastructure is not currently treated or identified as critical infrastructure for cybersecurity purposes. Should we rethink whether AI is actually critical infrastructure, and if so, what would that mean from a cybersecurity standpoint?

Mr. ANDERSEN. Thank you for your question.

The short answer is yes. The longer answer is we have lots of technologies that we previously considered critical infrastructure designations, things like cloud computing and artificial intelligence companies that were previously not considered to be critical infrastructure. Doing so today would give us an opportunity to examine minimum cybersecurity requirements; would bring them into the fold for larger strategic planning, and lash them up with communities like DHS's CISA, the Cybersecurity and Information—excuse me—the Cybersecurity and Infrastructure Security Agency, to be able to engage in information-sharing operations. These types of things would help to underpin greater security in these critical infrastructure industries.

Mr. FITZGERALD. Very good. Thank you.

Mr. Mohr, the stakeholders raised concerns about difficulties in protecting trade secrets during litigation. What is the standard process for protecting trade secrets in court cases, specifically?

Mr. MOHR. Well, typically, what happens is that there is a protective order, in other words, when the accused party has a right to defend themselves and they have a right to know, OK, what are they being accused of stealing? So, if it is a trade secret and it leaks out, for example, on a court docket, then the secrecy is gone and it's no longer valuable.

So, what the judge will do is balance a number of factors, and typically, write an order that restricts access to the trade secret and makes sure that the information doesn't leak out into the public domain.

Mr. FITZGERALD. Right. So, if the risk of trade secret leakage increases as the use of third-party litigation funding continues, especially like a patent case or other technology, what would be kind of the scope of the requirements in and around that?

Mr. MOHR. Well, it—

Mr. FITZGERALD. How do you protect yourself?

Mr. MOHR. Well, the scope is really left to the discretion of the trial judge. From our point of view, the more information the trial judge has, the better an order that the judge is going to be able to write.

So, for example, suppose you knew that one of the parties—let's take this: It's a third-party litigation-funded lawsuit. It is a party that is funded by the Chinese government. If you're the judge and you're crafting a protective order in that case, you would write a pretty—you'd probably write a much more severe one than if you thought it was just a couple of local dry cleaners fighting over a formula. That protective order might be very, very different.

You might have, for example, personal liability for the attorneys, which has a way of focusing the mind, if any of the information

were to leak out. There's a number of things. The judge can put protocols into how, in terms of how the information is used; how it's stored; under what circumstances; and who can see it, and how that access is logged, among other things.

Mr. FITZGERALD. Very good. Thank you.

Dr. Villaseñor, why is trade secret protection important to AI development compared to just any other type of IP protection? I guess, specifically, many of us heard testimony this morning, between the United States and China as well. Why is that? Why is it important?

Mr. VILLASEÑOR. Well, trade secrets are important across the spectrum of industries, but they are absolutely critical to AI. Because even in the case of—you might have heard these systems that are described as open systems, the open AI systems. There are still enormous amounts of trade secrets that go into that.

In other words, if somebody releases the model weights, for example, as open, they wouldn't necessarily release how they trained those model weights and what the training aid that was used. They're not going to often release the source code.

There's an enormous amount of trade secrets in AI, just like there are in other areas as well, but with AI, it's particularly complex, just because of the sheer size and magnitude of these systems is so large, that there's just more opportunity to build an incredible amount of trade secrets.

Without trade secrets, we do not have the ability to maintain our AI leadership. That's what the investment is going into and that's what the companies are being valued for.

Mr. FITZGERALD. I'm guessing, because China is so secretive in the way they have, the way they view this, that it makes it even more difficult when it comes to, specifically, seeing exactly what they're up to, is that correct?

Mr. VILLASEÑOR. Well, the open system that we have here, where companies make their own choices about what to reveal and what to keep secret, is incredibly powerful. The proof is in the pudding. We are, unquestionably, the country with the leading AI ecosystem, and I don't think that's an accident.

Mr. FITZGERALD. Thank you, Chair. I yield back.

Mr. ISSA. I thank the gentleman.

We now recognize the Ranking Member of the Subcommittee, the gentleman from Georgia, for his opening—his questioning.

Mr. JOHNSON. Thank you, Mr. Chair.

Ms. Toner, the prospect of ceding American technological leadership to China is often used as an argument against implementing regulations of any kind on AI. Do you agree with that approach?

Ms. TONER. No, I do not believe that we should say that the need to beat China necessarily means that we cannot regulate AI ourselves for several reasons.

The first and most important reason is that regulation does not actually need to slow down our industry whatsoever. Well-designed regulation can actually even support industry. So, AI is an industry where there are huge problems with consumer trust right now. There's been some data showing that products that list that involve AI will actually be trusted less by consumers, because consumers

are used to experiencing these hallucinations and reliability issues that we have with AI.

So, I think there are ways in which, if you can use regulation to build consumer trust by making them know that they're going to be interacting with high quality products, and likewise, know that they are going to have recourse if something goes wrong; know that they are not just out there on their own, that actually can be very industry-boosting.

So, that would be a primary reason that this is not a good argument. People making this argument that we can't regulate because we might then lose to China, also tend to neglect the pretty hefty regulations that China is enacting on its own AI ecosystem, and also, sometimes overestimate the quality of the training of the AI ecosystem, which is certainly competitive with the U.S., but not poised to overtake and run far away from us anytime soon.

So, no, it's really important to protect our citizens, to uphold our democratic institutions and way of life, and also, to support the industry itself that we put in place—smart guardrails.

Mr. JOHNSON. Uh-hum. What makes you so confident that China is not poised to overtake the United States in AI development? What are some of the ways that regulations can hurt the pace of innovation in America, AI innovation in America?

Ms. TONER. Sure. I'll take the questions in reverse order.

I think AI is a rapidly developing technology. If we were to go ahead and try and create regulations that were sort of a checklist of, if you're building AI, you have to do these 12 steps that a government committee came up with, and then, they don't get changed and they don't get adapted. They're not responsive to specific cases.

Regulations that really are very prescriptive and limit what companies can do or force them to use procedures that would not be competitive, that would not be productive. So, we should not be going that route.

There are many other kinds of approaches. So, for example, looking at transparency and disclosure, that doesn't need to force you to build your systems in any particular way; simply share information about what you're doing.

To your first question about Chinese competitiveness, this may be an area where I differ a little from some of the other witnesses present today. Honestly, the biggest advantage that the U.S. has right now is our access to compute, so computational power and advanced AI chips.

The export controls, while they have been imperfectly applied and imperfectly enforced, they have been a huge success, or at least have the signs of being a huge success, if we carry out—if we continue to enforce them and keep them in place.

One example of a signal for this is that the CEO of DeepSeek has made very clear that access to compute is the biggest limitation for him. So, the way that they were able to train the system that made such a splash was using a large number of chips that they imported in the gap between an October 2022 set of export controls, and then, they bought a bunch of chips throughout 2023. Then, in 2023, those chips were also restricted. So, they are now no longer able to buy the kind of chips that they used to train that system.

So, the way that the export controls work is not just a matter of a few of them get slipped through? It's really a question of the volumes that we are able to produce outside of China.

We need to also be looking at the semiconductor manufacturing equipment. That's a huge piece that often gets neglected. So, this is not just preventing of the chips themselves, but preventing the machines, the exquisite, very expensive machines that are produced in a very small number of countries that are U.S. allies. Preventing those—actually, enforcing the protections on those would also help protect the U.S. advantage.

So, I'm happy to have a longer conversation about the export controls but I think that is a huge advantage right now.

Mr. JOHNSON. Thank you. Dr. Villasenor, would you agree that not only AI transparency obligations implicate trade secrets?

Mr. VILLASENOR. Yes. That's, that's true. There would be some that would not, but many would, and some that don't.

Mr. JOHNSON. Is there a way to craft policies such that the disclosure requirements necessary for transparency can avoid touching on trade secrets?

Mr. VILLASENOR. In general, it is possible, but it probably depends on the sector. AI spans all these sectors. So, the answer can be different depending on the specific sector.

Mr. JOHNSON. Thank you. I'm out of time. I yield back.

Mr. ISSA. The gentleman yields back.

We now go to the gentleman from Kentucky for his questioning.

Mr. MASSIE. Thank you, Mr. Chair.

Which of the witnesses is proposing that the government should take some kind of action? Raise your hand.

[Show of hands.]

Mr. MASSIE. OK. Ms. Toner, what is, what is the action that you think the government needs to take?

Ms. TONER. So, I have several suggestions. Perhaps a top priority would be to expand the current voluntary collaborations that are being undertaken between national security parts of the U.S. Government and the U.S.'s leading AI companies.

So, there's some early efforts right now. They include threat intelligence-sharing with the intelligence community. So, they are working hand-in-hand, in similar ways to how they do with critical infrastructure providers or our Defense Industrial Base, to ensure that, when there are incoming threats—and we do have State-based actors trying to infiltrate our U.S. companies—they are trying to find unclassified ways to ensure that the companies are aware and can prevent those threats and defend against them.

There's also very valuable collaborative testing going on—

Mr. MASSIE. Which direction is most important: The government sharing information with the companies or the companies sharing information with the government?

Ms. TONER. They're both very important. Perhaps if I had to pick one, I'd say the government sharing information with the companies, but there has also been valuable threat reporting from the companies as well.

There's also been within the Department of Commerce a dedicated institute, the AI Safety Institute, that has been, again, on a voluntary basis, working with some of these leading companies to

test their new, most advanced systems. So, these are systems where the companies themselves say, "We think they might soon be able to aid in the creation of bioweapons." They might soon be able to help not very sophisticated hackers hack into U.S. critical infrastructure. They might pose other threats. There are ways in which having access to classified information and classified expertise allows the government to actually help those companies do tests that they want to be doing anyway.

Mr. MASSIE. Do you think the collaboration should be compulsory?

Ms. TONER. No, most likely not. It should certainly be resourced, authorized, and expanded.

Mr. MASSIE. Dr. Jensen?

Mr. JENSEN. I guess you were seeing in my eyes I'm more of the small government guy.

We are seeing broad agreement on a number of things.

Mr. MASSIE. You did raise your hand.

Mr. JENSEN. I did a little tipsy-tipsy.

Mr. MASSIE. OK. Yes.

Mr. JENSEN. We do have—

Mr. MASSIE. Which concerns me.

[Laughter.]

Mr. JENSEN. Well, but—

Mr. MASSIE. Just kidding.

Mr. JENSEN. We'll settle it over—

Mr. MASSIE. I'm interested in your answer.

Mr. JENSEN. Yes. So, I would say this: You have broad agreement about the need to provide cybersecurity. Now, whether that's an incentive from the government, and then, there's some minimum viable standard that industry is held to, or whether there's more of a government can reach in and monitor everything from the employees to the company, to push someone—what becomes voluntary sharing becomes "voluntold" sharing.

So, I would tend to think we agree on quite a bit here, but let's talk about that split difference. Because showing our differences is important for you all as a Committee.

I would say I tend to think that smaller, lesser government is what's important, because that's what actually allowed these companies to grow, these companies to thrive.

Now, we have to balance that against that you have a large predatory communist State that is directly targeting them. So, there's a question of, what is the Federal Government's national security obligation to protect U.S. persons and companies versus not overreaching with regulation to have them spending the marginal dollar to hire attorneys or to invest in some system that they're not spending in the lab trying to develop a new edge to the frontier model or some new component?

That is a really hard balance to strike. I don't envy your job, but I'm glad you're all going to do it. Because it means the basic protections, that even the *Federalist Papers* we're talking about. It means thinking about, what does it look like to declassify sensitive intelligence information, where we document this, so that it's admissible in our courts, or in courts in other free societies?

So, what you're seeing is we broadly agree on the need to help companies help themselves with cybersecurity. We broadly agree that the Federal Government has a role. We might disagree with the extent of that role. Then, we also agree that these companies really are going to define our economic growth and prosperity into the coming century.

Mr. MASSIE. I have another question. Probably, Dr. Villasenor, you might be the one to answer this. Are AI companies looking to use trade secrets because patents aren't necessarily conducive to protecting their Indo-Pacific?

Mr. VILLASENOR. Well, it's a great question. There is a subset of innovations that could be protected either as trade secrets or patents, but trade secrets have a far broader scope. They can protect far more. There are plenty of things that are protectable by trade secrets. For example, long lists of files of source code; you can't just get a patent on a million lines of source code. That source code is certainly a trade secret.

There's an enormous amount of intellectual property that is not protectable as a patent, but that is, nonetheless, vital to the value and value proposition and differentiation of the company.

Mr. MASSIE. Isn't the biggest trade secret risk here is somebody just comes in and hires the employees?

Mr. VILLASENOR. Well, I would hope that employees would respect their confidentiality obligations. It is certainly the case that we have had problems—there have been problems like that. That's one risk. There's hacking. There are many risks to trade secrets.

Mr. MASSIE. Thank you.

Thank you, Mr. Chair. I yield back.

Mr. ISSA. Thank you.

We now go to the Ranking Member of the Full Committee, Mr. Raskin, for his questions.

Mr. RASKIN. Thanks, Mr. Chair.

Continuing with you, Dr. Villasenor, many of the AI models incorporate open-source code, coding that's publicly available, into their models. How does this affect their ability to assert a trade secret claim?

Mr. VILLASENOR. Well, it's a very good question. It depends in part on how they've incorporated these open-source sources, for example. It is certainly possible to have a system that has some component that was based on open source, but that also has a lot of intellectual property that's created independent of that, and there would be trade secret value in that and, for example, in how they integrate that with open source information.

So, I wouldn't conclude, or I wouldn't believe that the presence or the use of open source would eviscerate trade secret rights for the companies that use it.

Mr. RASKIN. All right. Dr. Jensen, do you agree with that you can still maintain some kind of trade secret, some actionable trade secret claim, even if you've been using open-source code as part of your programming?

Mr. JENSEN. It's hard, and this is why, again, I want to stress that idea of going on with the offense. This is where it definitely gets outside the jurisdiction of this Committee and gets really into what's the rights of the Executive.

You are going to have to find ways to potentially sabotage the most malicious offenders that you identify as linked to a foreign government going after you. Because you can protect it, he's right, with a larger trade secret, then, it becomes only a matter of time before they put the pieces together.

If you have someone engaged in industrial-size, like generation-defining theft, you can't trust that person. So, where is the balance there of how you actually take other measures that are, again, outside this jurisdiction to start to hold those companies—countries accountable, and then, undermine it? That's the only way I think it's going to work.

Mr. RASKIN. OK. Ms. Toner, you've advocated for transparency requirements for developers of high-stakes AI systems, including transparency for training data, capability testing, safety testing, risk management, safety cases, and so on. What does transparency mean in this context? What is its purpose in these different areas?

Ms. TONER. It's a great question. I would just clarify I would not necessarily advocate for transparency over training data, but the rest of the items that you listed, certainly.

There's different purposes and different forms it can take. The simplest form of transparency is transparency to the public. This has a very broad range of benefits. It means that it's already transparent to governments, because governments can access anything that is public, but it also lets a broader set of academics, experts, employees of companies who might be affected—it just really empowers the public to understand the stakes of this technology and how the technology is changing over time, which I think is important, given that it is going to affect all our lives very profoundly and perhaps in sudden and unexpected ways.

A different kind of transparency is transparency to government. So, there's some information that maybe is not suited to be public. Maybe we want to keep them protected.

Mr. RASKIN. Uh-hum.

Ms. TONER. That could particularly be relevant for national security-relevant information. So, for example, a big area of concern right now is the potential cybersecurity capabilities of the most advanced models, whether they're going to make critical infrastructure systems more vulnerable than they have been in the past. Maybe that's not something that we want disclosed publicly immediately, but it is an area where partnership with government makes sense.

A third form of transparency, which is maybe transparency, is not quite the right word, but it's important to also think about the ability to bring in independent third parties into these companies and provide independent oversight or independent verification of some high-stake claims they're making. So, if they are saying that they are running certain kinds of tests, that they're performing certain kinds of safety protocols, can you bring in a third party under an NDA to work inside the company's own facilities? That might allow you to get a little bit of additional independent verification, so you're not just taking the company's word for everything for these high-stake claims they're making.

Mr. RASKIN. Great. Thank you.

Dr. Jensen, *The Washington Post* reported that tech companies, or some tech companies are telling their employees on visas not to leave the United States, out of concern that they won't be readmitted to the country or they could be stopped at the border. Visa holders are, obviously, running a lot of tech companies. They're working at startups. They're key in the field. Seventy percent of graduate students in AI-related fields are believed to be international students.

So, if the Trump Administration begins to deny H-1B visas, as he did in the first term, what will the consequences be on American AI innovation and on these businesses?

Mr. JENSEN. Well, I'll start with this combat veteran. It will cut my lab in half. Literally, the three people I employ, I would cut it to four people, counting me, total—I would lose two of them. I'm a microcosm compared to the size and scale of how those could ripple through the American ecosystem.

That doesn't mean that we don't have the right, and the Executive doesn't have the right to determine how best we seal our borders and determine very complex immigration questions, but we have to have a really hard conversation, as a Nation, about what really is the major competition of the 21st century.

If it truly is AI, and AI becomes the focal point of grand strategy, that means immigration discussions have to be taken as part of that, and we're going to have to find some areas of bipartisan agreement or compromise. Then, we're going to have to really double-down in investment in STEM education, which is going to even take longer, and we have to figure out how it works.

Now, I'd just say one note quick about transparency to double-down. There's a really interesting point of transparency. So, in my lab, we do benchmarking. You're going to need almost a Tocquevillian civil society function where, whether it just naturally happens or it's incentivized by the people's house, independent groups—not government, not business—come together and hold company models accountable.

So, in our case, we actually do the hard work to say, when a DeepSeek or a Gemini responds with escalatory responses on a dataset trained on standard international relations and foreign policy decisionmaking, that's just one example.

So, it's not just transparency in the ways we've discussed. It's also let's get creative and think about all American society, and what are the ways civil society can be incentivized to organize organically from below and provide checks on us? Because I don't think benchmarking can just be the government; that will lead to overreach. It can't just be companies because that will lead to kind of skirting claims. There's just—there's perverse incentives for either the government or just firms. So, transparency needs to also include civil society and us thinking about, what does that benchmarking look like, conducted through voluntary American associations?

Mr. RASKIN. I appreciate that. I yield back, Mr. Chair.

Mr. ISSA. That was a great round of questioning. I appreciate it. I appreciate your answer on broadening transparency.

With that, we go to the gentleman from South Carolina, Mr. Fry.

Mr. FRY. Thank you, Mr. Chair. Dr. Jensen, to continue with you, you would agree that AI is one of our most critical tools in strengthening national defense?

Mr. JENSEN. One hundred percent.

Mr. FRY. In that same vein, would that translate, if we were a leader in that, would that translate to superiority for our defense capabilities and our warfighters on the battlefield?

Mr. JENSEN. A great question and I can tell you honestly. So, as the chair at Marine Corps University for the last 2½ years, we've been experimenting with how could you use AI to help marines plan better. So, no more eating crayons. Time to actually get down with the code.

Frankly, we found tremendous strides. This is actually why it's a complex answer to this. It's not just a function of the engineering; it's how you actually change professional military education and training to make officers and enlisted personnel understand that technology and to know how to ask the right question.

What makes us the best fighting force is that we care about our people. We invest in them. We challenge them. We pull them from all ranks of our society.

In an era of AI, that also means ensuring they have the requisite technical education, and we've given them the ability to work with algorithms to augment military decisionmaking.

So, it won't just be enough to be an AI superpower and to give a trillion dollars to one company to give us widgets. It's going to be the harder investments we make in our people, how we change our training pipelines, and how we simulate future battles.

Mr. FRY. So, to what extent do you think that Chinese espionage is undermining our national defense capabilities in the space of AI?

Mr. JENSEN. Yes. Daily, if not every second. Remember, they have proven that you can mass steal your way into the 21st century through intellectual property theft, both with hackers, but also, we heard about it today: These third-party purchases of firms, through insider recruitment. They've got a deep, well-established play book.

(1) That changes our cost to innovate. Every secret they steal changes the marginal cost for the next innovation. It's cheaper for them, more expensive for us.

(2) It also gives them sensitive data on how best to defeat our systems. So, this is why we have to probably come up with entirely new concepts of how we secure data and how we secure training data. Because the worst thing we would want is they actually steal every experiment we've done with AI in a military training setting and, actually, statistically analyze our patterns.

Most people, when they're fighting, have tells. Boxers know this, but it's true at larger-order combat formations. We all have patterns, and if you can see the enemy's pattern, you can conduct a spoiling attack or some maneuver to offset it. We have to make sure they can't use our patterns through seeing us in that technology to exploit in the battlefield.

Mr. FRY. Well, how do we do that? In dealing with espionage of trade secrets—

Mr. JENSEN. Yes.

Mr. FRY. —what kind of protection do you think would be most important toward that kind of incursion by the CCP?

Mr. JENSEN. This is where the lawyers—don't get mad if I say this.

[Laughter.]

Mr. JENSEN. I'm going to put my warfighting hat on.

First, we probably have to get really creative with almost creating entire digital terracotta armies. Why shouldn't it be that every U.S. military personnel isn't in three to four places simultaneously, only one of which is real? So, your adversary, even if they can see you in a transparent global competition, doesn't know what's real.

It means we're probably also going to have to get pretty aggressive with data poisoning, knowing full well that there's real risk of that blowing back on us, given how these models are trained.

These are really the core counterintelligence and operational security questions of the 21st century. That doubles back to, if you don't train your intelligence community and your warfighter how to answer these questions, we're never going to develop policies in the military, and then, we're going to have generals testifying before you who don't know what they're talking about. Now, we can do better than that and our military will do better than that, but it requires that technical training, that pipeline, that space to experiment.

Mr. FRY. Thank you for that.

Ms. Toner, can you briefly explain China's Thousand Talents Program? Does it specifically target U.S. scientists and AI professionals?

Ms. TONER. So, the Thousand Talents Plan is only one of many, a very large number of talent plans that China uses to try and recruit talent in critical industries. They certainly target AI with the Thousand Talents Plan and other plans, and they're certainly making the most of the current administration's effects on U.S. immigrants in the United States.

So, there's a lot of interest among people who are currently here in visas, in whether their future in the U.S. is secure. You can bet that China is making the most of that, both with plans like Thousand Talents and, also, offering lots of resources for research—great, cushy jobs. They're, they're certainly stepping in there.

Mr. FRY. Do you think that those recruitment efforts have led to the leakage, if you will, of trade secrets or sensitive technologies from the United States and other Western countries?

Ms. TONER. Certainly, in the AI industry broadly, as has already been mentioned, one of the biggest sources of trade secrets being leaked is simply employees moving from one company to another. This happens inside Silicon Valley between Google and OpenAI, and other similar companies. Certainly, if you're able to hire employees from those companies and get them to cover over to China, that's going to have the same effect.

Mr. FRY. What can we do to close that security gap, just briefly? I know my time is expired, but I wanted to get to that.

Ms. TONER. One piece here would be, for people who are doing it intentionally and are doing it maliciously, that is where some of my recommendations around personnel vetting could come in. It's

very important that this not become a broader anti-immigrant sentiment, though. Because, as Dr. Jensen has already laid out, the contributions of foreign nationals to U.S. AI competitiveness are immense.

Mr. FRY. Thank you for that.

Mr. Chair, I yield back.

Mr. ISSA. I thank the gentleman. We now go to the gentlelady from North Carolina, Ms. Ross.

Ms. ROSS. Thank you, Mr. Chair and Ranking Member, for holding this hearing.

I apologize for being a little late, but we had a hearing on quantum computing that raised many of these same issues.

Mr. ISSA. The best part is you arrived just in the nick of time.

Ms. ROSS. Yes, there you go. Anyway, Dr. Jensen, DeepSeek's rapid AI advancements have sparked debate. I wanted to know whether you think they are driven by local innovation or replication or theft of American research. Where do you think they come from?

Mr. JENSEN. It's straight-up stealing. We can give different verbs to describe theft, but it's how they did it that's important for us to provide the right type of protection.

So again, the idea is, if I'm going to, basically, do these attacks where I exploit your ability to pull data and ask a question to one model, to shorten the amount of time and the amount of computational cost to train my model, it's at minimum a legal gray area, but I really do think it's that. I defer to the legal experts on that.

What's more important about DeepSeek to take stock of is I think stealing in the 21st century, as awful as it is still subject to diminishing returns, and why we can still win and will continue to.

I say that because of our benchmarking study, we tested DeepSeek. DeepSeek was actually prone toward escalatory responses in a foreign policy scenario, so 66,000 unique question-and-answer pairs and 400 scenarios. Even worse, it was horribly biased against the U.S. and the U.K. Now, you might say that's a mirror into Chinese Communist Party leadership, but any mirror like that has a bias, is actually a weakness we can exploit over time.

So, that's why benchmarking becomes so important. Because you want to understand the tendencies in these models, and then, an open society with an open market, there will be commercial incentives to update those models. Whereas, a closed society excels only at lying to itself, and that's actually going to put them in a strategic deficit.

Ms. ROSS. Thank you.

Ms. TONER. Can I comment on that as well?

Ms. ROSS. Oh, absolutely.

Ms. TONER. Yes, I apologize, but just to respectfully disagree with the assessment of what DeepSeek did here. I think it's really important.

There has been plenty of overstating of the sophistication of what they did and how advanced their AI system is, but it doesn't help us to understate it, either. It's important to describe what it is believed that they did in terms of distillation, which is the technique they used.

This is a very common technique that a lot of U.S. AI developers will use as well. Essentially, it's using a more advanced AI model to get some answers and to use that as part of your training data.

I don't have any inside information. We'd have to look at the internal investigation OpenAI is running. What's available externally suggests that they have just done a pretty regular standard practice procedure as one small part of their overall process for building this model.

It's important that we not underestimate the level of engineering sophistication and research that they did bring. They were genuinely innovating here, in addition to making some use of OpenAI's models, I believe, according to evidence we have—again, in a way that I think is a legal gray area is correct, a legal gray area and very commonly done by many U.S. AI developers as well.

Ms. ROSS. Thank you for that addition.

Back to you, Dr. Jensen. Drawing from your analysis of technology diffusion, what indicators, patent citations, talent flows from U.S. labs, or code-based similarities would signal reliance on external knowledge versus organic R&D in China?

Mr. JENSEN. So, I love this question because you're getting at the heart of what does it mean to be an AI superpower, and how would you measure it? Then, how could you, as elected officials, look at those measures and determine the right mix of legislation, or even the right type of budget allocations to go forward with.

A few stand out, even before whether it's externally or internally driven.

First, triad patents, absolutely, are always going to be a key one.

Second, even though we can't necessarily always draw a direct link, even if there's a correlation, I do think STEM education is critical, as well as basic research investments.

There are certain categories of research, frankly, that it's just not commercially viable for companies to invest in. In fact, most of our more interesting technological developments, really in the kind of post-World War II, Vannevar Bush moment, come from our willingness to take risks and basic research on universities, and then, finding the right type of—whether it's protecting it with patents, but then, also, commercial incentives for those researchers, and then, entrepreneurs to roll those out.

So, one of the real measures will be those things, in my opinion, and then, you'll know if it's really coming up. There's only so much of that you can steal.

Ms. ROSS. So, we just came—I just came from the Science Committee, and we are actually seeing NSF grants being canceled if they have, quote, "DEI connection," which, to me, is a way of canceling investment in talent in underserved communities, because we have talent everywhere in the United States. Could you comment on that?

Mr. JENSEN. Sure.

Mr. ISSA. Briefly, if you would, please?

Mr. JENSEN. Yes, I'll be very quick.

For me, first, it starts with basic research. True DEI in this case means we just really want good researchers, and you're right, they come from everywhere.

The debate here would be whether trying to preface certain communities inadvertently undermines the commitment to treating everybody by the content of their character, not by the color of their skin.

My first priority would be increasing that basic research investment, and then, figuring out how we make sure we have research ecosystems that are distributed across America, so we can find all that talent where it is.

Ms. ROSS. Thank you. I yield back. Thank you for your indulgence.

Mr. ISSA. I thank the gentlelady. No problem.

We now go to the gentleman from Virginia for five minutes.

Mr. CLINE. Thank you, Mr. Chair.

Mr. Andersen, trade secrets are often described as one of the most important tools for fostering innovation. In your view, how critical is the protection of trade secrets for the continued advancement of AI technologies, particularly in the context of U.S. companies trying to stay competitive with foreign players like China?

Mr. ANDERSEN. I believe it's exceedingly critical. Being able to safeguard the secret sauce, if you will, of how we're going about our business is exceedingly important.

I'm as antiregulation as I probably can be, but, when I left home and deployed to Iraq and left the wire to go out on patrol, I didn't look at having to put on a flak jacket and Kevlar and be conditioned with my rifle as an overly burdensome regulation. I looked at it as a recognition of the operating environment that I was in. Engaging in both good cybersecurity practices and being able to protect trade secrets is exceedingly important to maintaining our edge.

Mr. CLINE. Given China's rapid advancement in AI, what steps should the United States take to protect its AI innovations from theft or exploitation by foreign adversaries, especially considering the open AI ecosystem that may facilitate such activities?

Mr. ANDERSEN. So, first and foremost, it's engaging in good, good cybersecurity hygiene. I brought this up very briefly with regard to the earlier question about critical infrastructure. Our technology companies, whether it's an AI company or cloud computing companies or some of the more generic developers in the market, are critical infrastructure. Moreover, the information that they're producing today is critical to both our economic success and our national security.

So, good, basic cybersecurity hygiene, whether it's looking at CMMC and what we're doing with the Defense Industrial Base, or how it would apply within this industry segment, personnel screening and vetting, and again, outbound investment screening, making sure we're not, unwittingly or wittingly, investing in a way that's going to harm U.S. national security interests is critically important.

Mr. CLINE. As Congress considers AI transparency legislation, how do we strike the right balance between disclosing enough to ensure AI systems are safe and understandable without undermining the incentives for American companies to keep innovating?

Mr. ANDERSEN. So, that's exceeding tough to do, to the requirement for disclosure versus, again, keeping sort of your secrets in-

house. In my mind, you have to develop sort of redline thresholds of what information is important and what information needs to be disclosed, in particular, focused on those critical technology security areas that we've identified as high-risk. So, in my mind, it's about bounding things in that appropriate way, not necessarily asking for a full disclosure and full openness in a way that would degrade competitiveness within the environment.

Mr. CLINE. Are there lessons that you've learned from your experience in cybersecurity risk management that could inform disclosure frameworks that would be created for AI systems without compromising proprietary data?

Mr. ANDERSEN. Well, I think you—if you look at legislation that's existed for the past decade, things like CISA 2015, which has allowed for private industry to be able to share more openly with the government and participate in threat intelligence information-sharing, that's a good model.

Mr. CLINE. Now, that's up for renewal this year. Would you make any adjustments or changes or—

Mr. ANDERSEN. There are always opportunities for improvement, but I would certainly support its reauthorization, just to be completely honest, just because I don't want to have one more opportunity for a company's general counsel to whine to me about liability protection issues. Anything we can do to continue to encourage the private sector to share information is fantastic.

Mr. CLINE. Any other panelists want to comment on the reauthorization of CISA 2015 that is coming up this year? OK. Anyone?

[No response.]

Mr. CLINE. All right. Mr. Mohr, from the software industry's perspective, what trade secret protections are most critical to ensuring that American AI companies can continue to innovate without fearing intellectual property theft, especially by State-backed actors?

Mr. MOHR. Thank you for the question.

There are several areas where the trade secret doctrine can apply. It can apply to the algorithm itself. Professor Villasenor raised a very interesting, a really interesting point, for example, about how, if, for example, one of these algorithms were found not to be covered by the trade secret doctrine, because nobody understands it, basically, a black box, but it's something that was kept secret and kept for commercial advantage—that would be a legislative gap. That would be a problem.

It can apply to the algorithm; it can apply to the training data; it can apply to perhaps a specific configuration of the chips used, any number of pieces of the puzzle.

Mr. CLINE. Thank you. I yield back.

Mr. ISSA. I thank the gentleman.

Mr. Andersen, if I can briefly just ask one question. You noted you are going over the wire, through the wire, and wearing your armor. Isn't it true that not everyone wears the same amount of armor, and that in some cases, if you wear every piece that they manufacture, you won't be able to move sufficiently fast to accomplish the mission?

Mr. ANDERSEN. Yes, sir, that's absolutely true. I couldn't say, just because I'm going into potential armed engagements in Fallujah, that somebody who's a police officer here in D.C. should be walking

around with the same amount of body armor. There's still a potential threat engagement there, but the operating environments are different. The requirements need to be tailored to what, specifically, is going to be useful both for the operating conditions and the risk.

Mr. ISSA. I thank the gentleman.

The gentlelady from California is recognized for five minutes.

Ms. KAMLAGER-DOVE. Thank you, Mr. Chair, and I want to thank the Ranking Member.

This was a really interesting discussion. For me, it remains abstract if we're also not talking about the available human capital and the talent investment that is needed.

I have a young person getting ready to go to college. I have been talking to college students. I have actually been talking to a lot of engineers in this space who are worried about their prospects for employment and, also, their ability to stay here and to contribute to building our edge in AI.

Mr. Chair, I would like to submit for the record a January 14, 2025, White House AI Talent Report.

Mr. ISSA. Without objection, so ordered.

Ms. KAMLAGER-DOVE. It warns that international researchers may increasingly choose to work in countries like Canada or the U.K. due to visa uncertainty. We know that nearly 50 percent of noncitizen AI Ph.D.s face immigration challenges, and many are unsure if they will even remain here.

So, Ms. Toner, if we continue to make it harder for top talent to stay, what are the strategic risks to U.S. innovation and our ability to protect those innovations through trade secrets?

Ms. TONER. The biggest thing I would say is that talent is a huge, asymmetric advantage for the United States. We're in systemic competition with China and in different elements. We have different levels of advantage. The ability to attract the world's best and brightest is one of our very biggest and most asymmetric advantages over China.

They are graduating more and more Ph.D. students, master's students, and specialty students. They are vastly outstripping our ability to train domestic talent because their population is larger. If we're just using domestic talent, even if we should, obviously, be improving our K-12 education system, our high education system, but we can do that all we want; if we only use domestic talent, we cannot match them.

We're very fortunate, the number of people, the number of really brilliant researchers and engineers who want to come to the United States, if we'll only let them.

I would say, we look at the way that affects the U.S. AI ecosystem. Two-thirds of the top AI startups had an immigrant founder. More than half of the AI talent at the Ph.D. level in the United States is foreign-born. This is a big part of our ecosystem. We should treasure it. We should value it. We should let those people come and let them stay.

Ms. KAMLAGER-DOVE. Thank you so much.

Unrelated, I was having discussions with folks in my district about breast cancer research and finding cures. The folks that were actually at the center are immigrants. I just kept thinking to my-

self, OK, and now, we're demonizing this group of people that's actually working to try to figure out ways to save lives.

Even Dr. Jensen just said that good researchers comes from everywhere. They may come from everywhere. We want them to come here, and by golly, we want to stay here. Because we want to have the edge.

We cannot protect our edge in AI and cybersecurity, actually, without investing in the people and the institutions that are building the edge. I'm talking about colleges and universities that feel like they are under attack—the faculty, the curriculum, the prospective students, and the students that are there right now.

Given that between 40–60 percent of AI-related master's degrees and nearly 60 percent of AI Ph.D.s have gone to non-U.S. citizens in recent years, I'm going to say to you, Professor Villasenor, what are the long-term risks to U.S. innovation if we keep pushing out the very talent that is being used to build this field?

Mr. VILLASENOR. I think the risks are enormous. I think we are leaders in AI in large part because of our human capital. As has been said by multiple people here, our human capital is people who are at least half, and probably a lot more, from overseas. We need to make sure to create a climate where they feel that they can stay here and start their businesses here. Because the businesses they start are going to be the ones that employ 100, 1,000, or 10,000 people in the future. They're going to start those businesses somewhere and we want it to be here.

Ms. KAMLAGER-DOVE. Thank you for that.

As I mentioned, I know we are talking about cybersecurity and cyber threats. I'm also thinking about all the other ways where AI can play a positive and constructive part in how we are coming up with solutions; how we are protecting our people; how we are enhancing our national security.

What should be most important is what folks bring to the table rather than what they look like or where they were born. I don't think a solution cares too much about the person who came up with it. We're interested in how we can build our competitive edge; how we can protect the folks in our country; how we can create more jobs; how we can create an ecosystem that is both safe and sustainable—right? Economically and politically, from a national security standpoint.

I'm just saying this because I'm talking to all the young people who are graduating, who want to play a role in how we are finding solutions for all these issues, and they are scared. We don't want folks to be scared. We want folks to feel hopeful and engaged, and like they're able to work with their country on addressing some of these solutions.

With that, Mr. Chair, I yield back.

Mr. ISSA. I thank the gentlelady.

I would only opine that you may be making a case for us to bring back up the H-1B reform, so that we are, in fact, recruiting and retaining the best and the brightest, as you noted.

With that, we will not go to that, gentlemen. I guess it boils down to me now. I will recognize myself for a series of questions.

One of the questions I have is—I will followup on the recruit and retain. It was opined by people on both sides of the dais that we may be losing good people under current policy.

For all of you, isn't one of the loopholes in our system that the massive amount of people who are training on AI, getting their degrees in AI, they go back to China? Isn't that effectively—the people at your university, you include Chinese exchange students who will train on AI, will be advanced by looking at what we're doing, and then, they will, whether they want to remain or not, be forced to return to China? Isn't that a practical reality today?

Ms. TONER. So, in fact, this is a great question and an important question, and it's one that colleagues of mine at CSET at Georgetown have done great work on.

Actually, if you look at the numbers, specifically, in AI and, specifically, for Chinese immigrants, and you look at how, what percentage of those researchers are staying over five years, over 10 years, the numbers are North of 85 percent. So, there's actually a very, very large fraction who do stay in the country.

Mr. ISSA. Yes, but under the current, under the current law—

Ms. TONER. Yes.

Mr. ISSA. —they are circumventing their original presence to do it. They are marrying an American. They are applying for this visa or that visa.

Yes, many people who come here who are the best and the brightest remain, but they don't come under a status that guarantees they remain. They take an undergraduate degree, then a graduate degree, then a work program, and then another graduate degree. We all know that there are ways to stay here for a long period of time, and eight years is a blink in the back-and-forth at university.

The question is: How many people come here and have a reasonable expectation that they can remain here permanently, and thus, make the plans that might lead to loyalty? That would be a different question.

I have two service members here. Are you both current? Reservists? You're not?

Were you an officer, Mr. Andersen?

Mr. ANDERSEN. I was not.

Mr. ISSA. You are enlisted. So, I'm going to make one assumption.

Dr. Jensen, you currently hold at least a Secret security clearance, don't you?

Mr. JENSEN. That's true, Chair.

Mr. ISSA. OK. How many other people here hold security clearances today?

[Nonverbal response.]

Mr. ISSA. OK. For your security clearances, was there a background check?

Mr. JENSEN. Yes, and now, we're also subject to what's called continuous monitoring evaluation.

Mr. ISSA. As a result, one of the questions in that background is, are you susceptible to, in fact, being leveraged by a foreign power? Isn't one of the greatest foreign power leverages having family in a foreign Nation, particularly a hostile one?

So, isn't one of the questions that has—the genie that we have to let out of the bottle is, one of our challenges, by definition, is whether—you said you had two out of the four. If they are from China and their family is in China, they are subject to potentially being leveraged through their family. If they are from China, and for the 6, 8, 10, or 12 years, every day of their lives, they are potentially susceptible to being taken back to China. They are less likely to be reliable from a standpoint of keeping secrets secret.

Ms. Toner, wouldn't you even agree with that?

Ms. TONER. That is true and a concern for, I would say, a small fraction of the people in question here.

Mr. ISSA. We only need one to give away the secrets and the next bomb will not be stopped on its way in.

One of the questions that I have here today is, there's been a lot of discussion about, basically, foreign policy, immigration, and so on. From a standpoint of keeping our edge, tariffs will not keep our edge in AI, is that correct?

Mr. JENSEN. I think that's correct.

Mr. ISSA. Ms. Toner, one of the areas that you opined on positively was that our export controls have helped us keep that edge, correct?

Ms. TONER. Yes, sir.

Mr. ISSA. When we talked about cooperation, the very chips that we have export controls on trying to keep from leaving, every company that we want to have work in a collaborative way with our government to help keep secrets secret, to help have the level of cybersecurity, every one of them pretty much uses those chips, right?

Ms. TONER. Yes, sir.

Mr. ISSA. Maybe we can have a sense of consensus here for a moment. Isn't it fair to say that, although we want it to be cooperative, we want it to be voluntary, access to those very powerful chips that we will not let our enemies have, in fact, creates a bargain in which you really must work with the government to make sure that you are safeguarding the fruit of those very powerful chips. Is that fair to say?

OK. Seeing no disagreement, I will say we have gotten that.

I'm going to—this is one of those times in which I don't want to abuse the opportunity. The Ranking Member is going to let me have an extra minute or two.

I just want to close with a question that, hopefully, sets it up. This hearing was primarily about our current edge, where it is, and what we should do. There will be a lot of questions, both from Members who couldn't be here—myself, I couldn't be at the Science Committee. I'm going to be asking them a lot of questions on quantum.

Isn't one of the most important things we should be doing—and I want to bring together both sides and their questions; we should be figuring out how to recruit and retain from the entire world the best and the brightest, and create an environment in which they are safe and secure from being moved out of the United States. That we have the first step in developing the best technology, and then, continue in every way possible to make sure that those who

are our enemies will not, in fact, use the fruit of that to their benefit; *i.e.*, China? Is that all a consensus?

[No response.]

Mr. ISSA. The last one is, Dr. Jensen, you touched on one thing, and I just want to make sure I understood it. It is sort of a technical question.

This whole question of diffusion—we all understand that today's AI, various AI models, are being offered in some cases free as a service. What you alluded to that is part of DeepSeek—Ms. Toner, I'm sure you saw it, too—if we allow models to be used as a service, and if they can be a service to people outside of the country nefariously trying to get ahead of us, then don't we, in fact, provide the very need that we are trying to deny when we hold back chips?

Either one of you.

Mr. JENSEN. Yes, I'll just start, Chair, by saying, yes, but this is where it gets precarious, right? So, the thing, again, I was talking about was the unbounded consumption attack, so how to manipulate the API beyond just the knowledge distillation. Even if that is just a legal gray area, and U.S. people exploit it, it doesn't make it right.

So now, the question becomes, how do you make sure that this technology proliferates? Because everyone has talked about, whether it's breast cancer, weather, the really interesting next innovations are second order. It's how people begin to employ these models to solve other problems, and you don't want to limit that. At the same time, you want to limit its abuse.

This is why you need to really go on the offense, and why I want to be brutally clear when I say that. That means finding a way for sensitive intelligence to be declassified, to then differentiate between what's natural business competition and what's actually nefarious, and then, begin to make it admissible in not just the U.S., but also in multiple other free societies. It starts to create a compounding effect.

Even in the more extreme case, that's when you turn it over to a Presidential finding and you actually talk about what you might sabotage digitally overseas.

Mr. ISSA. Ms. Toner, you had a closing statement?

Ms. TONER. Yes. To build on that, a really important element here that often is not discussed as much as it should, is how these companies are monitoring the use of their systems. It's not just a question of testing them in advance or the cybersecurities at the companies themselves, which are very important. If you're going to make your products available to users, which is important for their business models; it's important for us to benefit from them, how are they detecting when they're being used improperly?

Different leading AI companies have different practices around monitoring different quality. I would certainly encourage you in your oversight role to discuss with the leading AI companies on how they are monitoring their systems being used.

I believe that OpenAI is currently investigating whether DeepSeek used their systems inappropriately, and if so, how? How do they detect that? What are they logging? What systems, automated and human-based, do they have in place to tell when those improper uses are occurring?

Mr. ISSA. Thank you.

Having no further questions from the dais currently, I would bring this to a close by saying that, for the next five legislative days, we will allow Members to ask additional questions. Would you all agree to respond to those in writing?

Then, just to make sure I don't miss anything on the close—nope.

Without objection, this hearing is adjourned.

[Whereupon, at 11:44 a.m., the Subcommittee was adjourned.]

All materials submitted for the record by Members of the Subcommittee on Courts, Intellectual Property, and the Internet can be found at: <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=118204>.

