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 2025[4] 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 "reapling] 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 Villasenor, *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 Thread 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 States[47] 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 Program[50] 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.").